Bitdefender®

INTERNET SECURITY 2015



MANUEL D'UTILISATION

Bitdefender Internet Security 2015
Manuel d'utilisation

Date de publication 16/07/2014

Mentions légales



Table des matières

INSTALLATION

1. PRÉPARATION DE L'INSTALLATION

Avant d'installer Bitdefender Internet Security 2015, procédez comme suit pour faciliter l'installation :

Vérifiez que l'ordinateur où vous prévoyez d'installer Bitdefender dispose de la configuration minimale requise.Si l'ordinateur ne dispose pas de la configuration minimale requise, Bitdefender ne pourra pas être installé, ou, une fois installé, il ne fonctionnera pas correctement, ralentira le système et le rendra instable.Pour des informations détaillées sur la configuration requise, veuillez consulter « *Configuration requise* » (p. 3).

Connectez-vous à l'ordinateur en utilisant un compte administrateur.

Désinstallez tous les autres logiciels similaires sur l'ordinateur.L'exécution de deux programmes de sécurité à la fois peut affecter leur fonctionnement et provoquer d'importants problèmes sur le système.Windows Defender sera désactivé pendant l'installation.

Désactivez ou supprimez tout logiciel pare-feu s'exécutant sur l'ordinateur.L'exécution de deux pare-feux à la fois peut affecter leur fonctionnement et provoquer d'importants problèmes sur le système.Le pare-feu Windows sera désactivé pendant l'installation.

Il est recommandé que votre ordinateur soit connecté à Internet pendant l'installation, même pour une installation à partir d'un CD ou DVD. Si des versions plus récentes des fichiers d'applications du package d'installation sont disponibles, Bitdefender peut les télécharger et les installer.

2. CONFIGURATION REQUISE

Vous pouvez installer Bitdefender Internet Security 2015 uniquement sur les ordinateurs fonctionnant avec les systèmes d'exploitation suivants :

- Windows XP avec Service Pack 3 (32 bits)
- Windows Vista avec Service Pack 2
- Windows 7 avec Service Pack 1
- Windows 8
- Windows 8.1

Avant d'installer le produit, vérifiez que votre ordinateur dispose de la configuration minimale requise.



Note

Pour connaître le système d'exploitation Windows de votre ordinateur et obtenir des informations sur le matériel, procédez comme suit :

- Dans **Windows XP**, **Windows Vista** et **Windows 7**, faites un clic droit sur **Poste de travail** sur le bureau, puis sélectionnez **Propriétés** dans le menu.
- Dans **Windows 8**, sur l'écran d'accueil Windows, localisez « Ordinateur » (vous pouvez, par exemple, taper « Ordinateur » directement sur l'écran d'accueil), puis faites un clic droit sur son icône. Sélectionnez Propriétés dans le menu inférieur. Regardez sous Système pour voir le type de système.

2.1. Configuration système minimale

- 1 Go d'espace disque disponible (au moins 800 Mo sur le lecteur système)
- Processeur 1,6 GHz
- 1 Go de mémoire (RAM) pour Windows XP, Windows Vista, Windows 7 et Windows 8

2.2. Configuration système recommandée

- 2 Go d'espace disque disponible (au moins 800 Mo sur le lecteur système)
- Intel CORE Duo (2 GHz) ou processeur équivalent
- Mémoire (RAM) :
  - 1 Go pour Windows XP
  - 1,5 Go pour Windows Vista, Windows 7 et Windows 8

2.3. Configuration logicielle requise

Pour pouvoir utiliser Bitdefender et l'ensemble de ses fonctionnalités, votre ordinateur doit disposer de la configuration logicielle suivante :

- Internet Explorer 8 ou version supérieure
- Mozilla Firefox 14 ou version supérieure
- Chrome 20 ou version supérieure
- Skype 6.3 ou version supérieure
- Yahoo! Messenger 9 ou version supérieure
- Microsoft Outlook 2007 / 2010 / 2013
- Microsoft Outlook Express et Windows Mail (sur les systèmes 32 bits)
- Mozilla Thunderbird 14 ou version supérieure
- .NET Framework 3.5 (automatiquement installé avec Bitdefender si manquant)

3. INSTALLER BITDEFENDER

Vous pouvez installer Bitdefender à partir du disque d'installation de Bitdefender ou en utilisant un programme d'installation téléchargé sur votre ordinateur à partir du site Internet de Bitdefender ou d'autres sites Internet autorisés (par exemple, le site d'un partenaire de Bitdefender ou une boutique en ligne).Vous pouvez télécharger le fichier d'installation sur le site Internet de Bitdefender à l'adresse suivante : http://www.bitdefender.fr/Downloads/.

Si votre achat protège plus d'un ordinateur (si, par exemple, vous avez acheté Bitdefender Internet Security 2015 pour 3 PC), répétez le processus d'installation et activez votre produit avec la clé de licence sur chaque ordinateur.

Pour installer Bitdefender à partir du disque d'installation, insérez le disque dans le lecteur optique. Un écran d'accueil s'affiche peu après. Suivez les instructions pour démarrer l'installation.



Note

L'écran d'accueil fournit une option pour copier le package d'installation à partir du disque d'installation sur un support de stockage USB.C'est utile si vous avez besoin d'installer Bitdefender sur un ordinateur ne disposant pas d'un lecteur de disque (sur un netbook, par exemple). Branchez votre périphérique USB, puis cliquez sur **Copier vers un disque USB**.Ensuite, branchez votre disque USB sur le PC ne disposant pas de lecteur de disque et double-cliquez sur runsetup.exe depuis le répertoire dans lequel se trouve le package d'installation.

Si l'écran d'accueil ne s'affiche pas, utilisez l'Explorateur Windows pour vous rendre au répertoire racine du disque et double-cliquez sur le fichier autorun.exe.

Pour installer Bitdefender à l'aide du programme d'installation téléchargé sur votre ordinateur, localisez le fichier et double-cliquez dessus.

Validation de l'installation

Bitdefender vérifiera d'abord votre système pour valider l'installation.

Si votre système ne dispose pas de la configuration minimale requise pour l'installation de Bitdefender, vous serez informé des zones devant être améliorées avant de pouvoir poursuivre.

Si un programme antivirus incompatible ou une version antérieure de Bitdefender est détecté, on vous demandera de le désinstaller de votre système. Veuillez suivre les indications pour supprimer les logiciels de votre système, évitant ainsi que des problèmes ne surviennent par la suite. Il est parfois nécessaire de redémarrer l'ordinateur pour terminer la désinstallation des programmes antivirus détectés.

Le package d'installation de Bitdefender Internet Security 2015 est constamment mis à jour. Si vous effectuez l'installation depuis un CD/DVD, Bitdefender peut télécharger les dernières versions des fichiers pendant l'installation. Cliquez sur **Oui** lorsqu'on vous y invite afin de permettre à Bitdefender de télécharger les fichiers, ce qui vous garantit d'installer la dernière version du logiciel.



Note

Le téléchargement des fichiers d'installation peut être long, en particulier sur des connexions Internet plus lentes.

Une fois l'installation validée, l'assistant de configuration s'affichera. Suivez les étapes pour installer Bitdefender Internet Security 2015.

Étape 1 - Bienvenue

L'écran d'accueil vous permet de choisir le type d'installation que vous souhaitez effectuer.

Pour une installation simplifiée, cliquez simplement sur le bouton **Installer**. Bitdefender sera installé dans l'emplacement par défaut avec les paramètres par défaut et vous passerez directement à l'Étape 3 de l'assistant.

Si vous souhaitez configurer les paramètres d'installation, cliquez sur **Personnalisé**.

Deux tâches supplémentaires peuvent être réalisées au cours de cette étape :

Veuillez lire l'Accord de licence de l'utilisateur final avant de procéder à l'installation. L'Accord de Licence contient les termes et conditions d'utilisation de Bitdefender Internet Security 2015.

Si vous n'acceptez pas ces conditions, fermez la fenêtre. Le processus d'installation sera abandonné et vous quitterez l'installation.

Activer l'envoi de **rapports d'utilisation anonymes**. Si vous activez cette option, les rapports contenant des informations sur votre utilisation du

produit seront envoyés aux serveurs de Bitdefender. Ces informations sont essentielles pour améliorer le produit et nous aider à vous offrir la meilleure expérience possible. Veuillez noter que ces rapports ne comportent aucune donnée confidentielle, comme votre nom ou votre adresse IP, et ne seront pas utilisés à des fins commerciales.

Étape 2 - Personnaliser les paramètres d'installation



Note
Cette étape apparaît uniquement si vous avez choisi de personnaliser l'installation lors de l'étape précédente.

Voici les options proposées :

Chemin d'installation
Par défaut, Bitdefender Internet Security 2015 sera installé dans C:\Program Files\Bitdefender\Bitdefender Internet Security 2015.Si vous souhaitez choisir un autre répertoire, cliquez sur **Modifier** et choisissez le répertoire d'installation de Bitdefender.

Définir les paramètres de proxy
Bitdefender Internet Security 2015 nécessite un accès à Internet pour l'enregistrement du produit, le téléchargement de mises à jour du produit et de sécurité, les composants de détection "in the cloud", etc.Si vous utilisez une connexion via un proxy au lieu d'une connexion Internet directe, vous devez sélectionner cette options et configurer les paramètres du proxy.

Les paramètres peuvent être importés à partir du navigateur par défaut ou vous pouvez les indiquer manuellement.

Cliquez sur **Installer** pour confirmer vos préférences et commencer l'installation. Si vous changez d'avis, cliquez sur le bouton **Par défaut** correspondant.

Étape 3 - Installation en cours

Patientez jusqu'à la fin de l'installation.Des informations détaillées sur la progression sont affichées.

Les zones critiques de votre système font l'objet d'une analyse antivirus, les dernières versions des fichiers d'applications sont téléchargées et installées

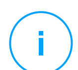
et les services de Bitdefender sont lancés. Cette étape peut prendre quelques minutes.

Étape 4 - Installation terminée

Un résumé de l'installation s'affiche. Si des logiciels malveillants actifs ont été détectés et supprimés pendant l'installation, un redémarrage du système peut être nécessaire.

Vous pouvez fermer la fenêtre, ou poursuivre la configuration initiale de votre logiciel en cliquant sur **Pour commencer**.

Étape 5 - Activer votre produit



Note

Cette étape apparaît uniquement si vous avez sélectionné « Pour commencer » à l'étape précédente.

Pour terminer l'enregistrement de votre produit, vous devez saisir une clé de licence.Une connexion Internet active est requise.

Procédez selon votre situation :

J'ai acheté le produit

Dans ce cas, activez le produit en procédant comme suit :

1. Sélectionnez **J'ai acheté Bitdefender et je souhaite l'activer maintenant.**
2. Saisissez la clé de licence dans le champ correspondant.



Note

Vous trouverez votre clé d'activation :

- sur l'étiquette du CD ou DVD.
- sur le certificat de licence.
- sur le courriel de confirmation d'achat en ligne.

3. Cliquez sur **Activer**.

Je n'ai pas de clé, je souhaite essayer le produit gratuitement

Dans ce cas, vous pouvez utiliser le produit pendant une période de 30 jours. Pour commencer la période d'essai, sélectionnez **Je n'ai pas de clé, je souhaite essayer le produit gratuitement**.

Cliquez sur **Suivant**.

Étape 6 - Configurer le comportement du produit

Bitdefender peut être configuré pour identifier automatiquement vos outils de travail afin d'améliorer votre utilisation dans certaines situations. Utilisez ce bouton pour activer ou désactiver les **Profils**.

Si vous travaillez, jouez ou regardez des films, activez les **Profils**. Cette action modifiera les paramètres du produit et du système afin de limiter au minimum l'impact sur les performances de votre système. Pour plus d'informations, reportez-vous à « *Profils* » (p. 18).

Cliquez sur **Suivant**.

Étape 7 - Enregistrer votre produit

Un compte MyBitdefender est nécessaire pour utiliser les fonctionnalités en ligne de votre produit. Pour plus d'informations, consultez « *Compte MyBitdefender* » (p. 41).

Procédez selon votre situation.

Je souhaite créer un compte MyBitdefender

Pour créer un compte MyBitdefender, suivez ces étapes :

1. Sélectionnez **Créer un nouveau compte**.

   Une nouvelle fenêtre s'affiche.

2. Tapez les informations requises dans les champs correspondants. Les informations fournies resteront confidentielles.

   Courriel - indiquez votre adresse courriel.

   Nom d'utilisateur - indiquez un nom d'utilisateur pour votre compte.

   Mot de passe - saisissez un mot de passe pour votre compte. Le mot de passe doit contenir au moins 6 caractères.

   Confirmer le mot de passe - saisissez à nouveau votre mot de passe.



Note

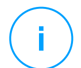
Une fois le compte créé, vous pouvez utiliser l'adresse courriel et le mot de passe indiqués pour vous connecter à votre compte sur https://my.bitdefender.com.

3. Cliquez sur **Créer**.
4. Vous devez terminer l'enregistrement de votre compte avant de pouvoir l'utiliser.Consultez votre messagerie et suivez les instructions de l'e-mail de confirmation envoyé par Bitdefender.

Je souhaite me connecter à l'aide de mon compte Microsoft, Facebook ou Google

Pour vous connecter avec votre compte Microsoft, Facebook ou Google, procédez comme suit :

1. Sélectionnez le service que vous souhaitez utiliser.Vous serez redirigé vers la page de connexion de ce service.
2. Suivez les instructions du service sélectionné pour lier votre compte à Bitdefender.



Note

Bitdefender n'accède à aucune information confidentielle telle que le mot de passe du compte que vous utilisez pour vous connecter, ou les informations personnelles de vos amis et contacts.

J'ai déjà un compte MyBitdefender

Si vous vous êtes connecté auparavant à un compte à partir de votre produit, Bitdefender le détectera et vous demandera de saisir le mot de passe pour vous connecter à ce compte.

Si vous avez déjà un compte actif, mais que Bitdefender ne le détecte pas, ou si vous voulez simplement vous connecter à un compte différent, saisissez son adresse e-mail et son mot de passe et cliquez sur **Se connecter à MyBitdefender**.

Remettre à plus tard

Si vous souhaitez remettre cette tâche à plus tard, cliquez sur **Plus tard**. N'oubliez pas que vous devez vous connecter à un compte pour utiliser les fonctions en ligne du produit.

INTRODUCTION

4. FONCTIONS DE BASE

Une fois Bitdefender Internet Security 2015 installé, votre ordinateur est protégé contre toutes sortes de malwares (comme les virus, les spywares et les chevaux de Troie) et les menaces Internet (comme les pirates, le phishing et le spam).

L'application utilise la technologie Photon pour améliorer la vitesse et les performances du processus d'analyse antimalware. Elle fonctionne en apprenant les modèles d'utilisation de vos applications système afin de savoir quoi analyser et quand, ce qui réduit l'impact sur les performances du système.

Vous pouvez activer la fonction Autopilot pour bénéficier d'une protection complètement silencieuse. Vous n'aurez ainsi aucun paramètre à configurer. Cependant, vous pouvez souhaiter profiter des paramètres de Bitdefender pour ajuster et améliorer votre protection.

Bitdefender peut vous permettre de travailler, jouer ou regarder des films sans être dérangé en reportant les tâches de maintenance, en supprimant les interruptions et en ajustant les effets visuels du système. Vous pouvez bénéficier de tout ceci en activant et en configurant les Profils.

Bitdefender prendra pour vous la plupart des décisions de sécurité et affichera rarement des alertes pop-up. Des détails sur les actions prises et des informations sur le fonctionnement du programme sont disponibles dans la fenêtre Événements. Pour plus d'informations, consultez « *Événements* » (p. 15).

Il est recommandé d'ouvrir Bitdefender de temps en temps et de corriger les problèmes existants. Vous pouvez avoir à configurer des composants Bitdefender spécifiques ou appliquer des actions préventives afin de protéger votre ordinateur et vos données.

Si vous n'avez pas activé le produit, pensez à le faire avant la fin de la période d'essai. Pour plus d'informations, consultez « *Activer Bitdefender* » (p. 39).

Pour utiliser les fonctionnalités en ligne de Bitdefender Internet Security 2015, veillez à lier votre ordinateur à un compte MyBitdefender. Pour plus d'informations, consultez « *Compte MyBitdefender* » (p. 41).

La section « Comment faire pour » (p. 48) vous fournit des instructions détaillées pour utiliser les fonctionnalités les plus courantes. Si vous rencontrez des problèmes lors de l'utilisation de Bitdefender, recherchez

dans la section *« Résoudre les problèmes les plus fréquents »* (p. 196) des solutions possibles aux problèmes les plus courants.

4.1. Ouverture de la fenêtre de Bitdefender

Pour accéder à l'interface principale de Bitdefender Internet Security 2015, suivez les étapes ci-dessous :

Dans **Windows XP**, **Windows Vista** et **Windows 7**:

1. Cliquez sur **Démarrer** et allez dans **Programmes**.
2. Cliquez sur **Bitdefender 2015**.
3. Cliquez sur **Bitdefender Internet Security 2015** ou faites un double clic sur Bitdefender B dans la zone de notification.

Dans **Windows 8** :

Localisez Bitdefender Internet Security 2015 dans l'écran d'accueil Windows (vous pouvez par exemple taper « Bitdefender » directement dans l'écran d'accueil) puis cliquez sur son icône. Vous pouvez également ouvrir le Bureau puis double-cliquer sur Bitdefender B de la zone de notification.

Pour plus d'informations sur la fenêtre de Bitdefender et l'icône de la zone de notification, reportez-vous à *« Interface de Bitdefender »* (p. 24).

4.2. Correction des problèmes

Bitdefender utilise un système de contrôle pour détecter la présence de problèmes pouvant affecter la sécurité de votre ordinateur et de vos données et vous en informer. Par défaut, il surveille uniquement un ensemble de problèmes considérés comme très importants. Cependant, vous pouvez le configurer selon vos besoins en sélectionnant les problèmes spécifiques que vous souhaitez surveiller.

Les problèmes détectés comprennent la désactivation d'importants paramètres de protection et d'autres conditions pouvant constituer un risque pour la sécurité. Ils sont regroupés en deux catégories :

Problèmes critiques - ils empêchent Bitdefender de vous protéger contre les malwares ou constituent un risque majeur pour la sécurité.

Problèmes mineurs (non critiques) - ces problèmes pourraient éventuellement affecter votre protection.

L'icône de Bitdefender de la zone de notification signale les problèmes en attente en changeant de couleur comme suit :

Des problèmes critiques affectent la sécurité de votre système. Ils requièrent votre attention immédiate et doivent être réglés dès que possible.
Des problèmes non critiques affectent la sécurité de votre système. Nous vous recommandons de les vérifier et de les corriger lorsque vous avez le temps.

Si vous faites glisser le curseur de la souris sur l'icône, une fenêtre de notification confirmera la présence de problèmes en attente.

Lorsque vous ouvrez la fenêtre de Bitdefender, la zone d'état de Sécurité de la barre d'outils supérieure indique la nature des problèmes affectant votre système.

4.2.1. Assistant de correction des problèmes

Pour corriger les problèmes détectés, suivez l'assistant de **Correction des problèmes**.

1. Pour ouvrir l'assistant, procédez comme suit :

   Faites un clic droit sur l'icône de Bitdefender dans la zone de notification et sélectionnez **Voir les problèmes de sécurité**.

   Ouvrez la fenêtre Bitdefender et cliquez dans la zone d'état de sécurité de la barre d'outils supérieure (vous pouvez par exemple cliquer sur lelien **Tout corriger !**).

2. Vous pouvez voir les problèmes affectant la sécurité de votre ordinateur et de vos données. Tous les problèmes présents sont sélectionnés pour être corrigés.

   Si vous ne souhaitez pas corriger un problème spécifique immédiatement, décochez la case correspondante. On vous demandera de spécifier pendant combien de temps vous souhaitez reporter la correction du problème. Sélectionnez l'option souhaitée dans le menu et cliquez sur **OK**.Pour cesser de surveiller cette catégorie de problème, sélectionnez **En permanence**.

   L'état du problème deviendra **Reporter** et aucune action ne sera adoptée pour corriger le problème.

3. Pour corriger les problèmes sélectionnés, cliquez sur **Corriger**. Certains problèmes sont corrigés immédiatement. Pour d'autres, un assistant vous aide à les corriger.

Les problèmes que cet assistant vous aide à corriger peuvent être regroupés dans les catégories suivantes :

Paramètres de sécurité désactivés. Ces problèmes sont corrigés immédiatement en activant les paramètres de sécurité correspondants.

Tâches de sécurité préventives devant être réalisées. Un assistant vous aide à corriger ces problèmes.

4.2.2. Configurer les alertes d'état

Bitdefender peut vous avertir lorsque des problèmes sont détectés lors du fonctionnement des composants de programmes suivants :

Pare-feu
Antispam
Antivirus
Mise à jour
Sécurité du navigateur

Vous pouvez configurer le système d'alertes afin de répondre à vos besoins spécifiques en choisissant les problèmes à propos desquels vous souhaitez être informé. Suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur l'icône en haut de la fenêtre et sélectionnez **Paramètres généraux** dans le menu déroulant.
3. Dans la fenêtre **Paramètres généraux**, sélectionnez l'onglet **Avancé**.
4. Cliquez sur le lien **Configurer les alertes d'état**.
5. Cliquez sur les boutons pour activer ou désactiver les alertes d'état en fonction de vos préférences.

4.3. Événements

Bitdefender tient un journal détaillé des événements concernant son activité sur votre ordinateur. Lorsqu'un événement concernant la sécurité de votre système ou de vos données a lieu, un nouveau message est ajouté aux

Événements de Bitdefender, comme lorsqu'un nouvel e-mail arrive dans votre boîte de réception.

Les événements sont un outil très important pour la surveillance et la gestion de votre protection Bitdefender.Par exemple, vous pouvez facilement vérifier qu'une mise à jour s'est effectuée correctement, s'il y a eu des malwares détectés sur votre ordinateur, etc.Vous pouvez également adopter d'autres actions si nécessaire ou modifier les actions appliquées par Bitdefender.

Pour accéder au journal des Événements, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur l'icône en haut de la fenêtre et sélectionnez **Événements** dans le menu déroulant.

Les messages sont regroupés en fonction du module Bitdefender dont ils sont liés à l'activité :

Antivirus
Pare-feu
Protection Web
Antispam
Safego
Optimisation
Vulnérabilité
Mise à jour

À chaque fois qu'un événement se produit, un point bleu apparaît sur l'icône en haut de la fenêtre.

Une liste d'événements est disponible pour chaque catégorie. Pour trouver des informations sur un événement spécifique de la liste, cliquez sur l'icône et sélectionnez **Événements** dans le menu déroulant.Des détails sur l'événement s'affichent alors dans la partie inférieure de la fenêtre. Chaque événement est accompagné des informations suivantes : une brève description, l'action que Bitdefender a appliqué et la date et l'heure de l'événement. Des options peuvent permettre d'appliquer une action supplémentaire si nécessaire.

Vous pouvez filtrer les événements en fonction de leur importance et de l'ordre dans lequel ils ont eu lieu.Il y a trois types d'événements filtrés en fonction de leur importance, chacun étant signalé par une icône spécifique :

- Les événements **Informations** indiquent des opérations réussies.

■ Les événements **avertissement** signalent des problèmes non critiques. Nous vous recommandons de les vérifier et de les corriger lorsque vous avez le temps.
■ Les événements **critiques** signalent des problèmes critiques. Nous vous recommandons de les vérifier immédiatement.

Pour voir les événements ayant eu lieu au cours d'une période donnée, sélectionnez la période souhaitée dans le champ correspondant.

Pour vous aider à gérer facilement les événements enregistrés, chaque section de la fenêtre Événements fournit des options permettant de supprimer ou de marquer comme lus tous les événements de cette section.

4.4. Autopilot

Pour les utilisateurs qui souhaitent que leur solution de sécurité les protège sans les interrompre, Bitdefender Internet Security 2015 dispose d'un mode Pilote automatique intégré.

En Pilote automatique, Bitdefender applique une configuration de sécurité optimale et prend pour vous toutes les décisions de sécurité.Cela signifie qu'aucune fenêtre contextuelle ni alerte ne s'affichera et que vous n'aurez aucun paramètre à configurer.

En mode Autopilot, Bitdefender corrige automatiquement les problèmes critiques, active et gère silencieusement :

La protection antivirus, fournie par l'analyse à l'accès et l'analyse en continu.

La protection pare-feu.

Protection Web.

Les mises à jour automatiques.

Pour activer ou désactiver la fonction Autopilot, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton **Mode manuel** / **Autopilot** sur la barre d'outils supérieure. Quand le bouton est sur la position Mode manuel, l'Autopilot est désactivé.

Tant que l'Autopilot est activé, l'icône de Bitdefender de la zone de notification est B.



Important

Lorsque le mode Autopilot est activé, modifier l'un des paramètres qu'il gère conduit à sa désactivation.

Pour afficher un historique des actions réalisées par Bitdefender alors que l'Autopilot était en cours, ouvrez la fenêtre Événements.

4.5. Profils et Mode Batterie

Certaines utilisations de l'ordinateur comme les jeux en ligne ou les présentations vidéo nécessitent plus de performance et de réactivité du système et aucune interruption.Lorsque votre ordinateur portable est alimenté par sa batterie, il vaut mieux que les opérations non indispensables, qui consomment de l'énergie supplémentaire, soient reportées jusqu'au moment où l'ordinateur portable sera branché sur secteur.

Pour s'adapter à ces situations particulières, Bitdefender Internet Security 2015 comprend deux modes de fonctionnement spéciaux :

- Profils
- Mode Batterie

4.5.1. Profils

Les profils de Bitdefender allouent davantage de ressources système aux applications en cours d'exécution en modifiant momentanément les paramètres de protection et en adaptant la configuration du système. L'impact du système sur vos activités est donc réduit.

Pour s'adapter à différentes activités, Bitdefender dispose des profils suivants :

Profil Travail

Optimise votre efficacité lorsque vous travaillez en identifiant et en ajustant la configuration du logiciel et du système.

Profil Film

Améliore les effets visuels et supprime les interruptions lorsque vous regardez des films.

Profil Jeu

Améliore les effets visuels et supprime les interruptions lorsque vous jouez.

Activer et désactiver les profils

Pour activer ou désactiver les profils, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Outils**.
3. Cliquez sur le module **Profils**.
4. Dans la fenêtre **Profils**, sélectionnez l'onglet **Paramètres des profils**.
5. Activez et désactivez les profils en cliquant sur le bouton correspondant.

Configurer Autopilot pour surveiller les profils

Pour une utilisation simple, vous pouvez configurer Autopilot afin qu'il gère votre profil actif. Dans ce mode, Bitdefender détecte automatiquement les activités que vous effectuez et applique les paramètres d'optimisation du système et du produit.

Pour permettre à Autopilot de gérer les profils, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Outils**.
3. Cliquez sur le module **Profils**.
4. Dans la fenêtre **Profils**, sélectionnez l'onglet **Paramètres des profils**.
5. Cliquez sur le bouton **Laisser Autopilot gérer mes profils** correspondant.

Si vous ne souhaitez pas que votre Profil soit géré automatiquement, ne cochez pas la case et effectuez la sélection manuellement dans l'angle supérieur droit de l'interface de Bitdefender.

Pour plus d'informations sur les Profils, reportez-vous à« *Profils* » (p. 189)

4.5.2. Mode Batterie

Le mode Batterie est spécialement conçu pour les utilisateurs d'ordinateurs portables et de tablettes. Son rôle est de limiter à la fois l'impact du système et de Bitdefender sur la consommation électrique lorsque le niveau de charge de la batterie est inférieur à celui que vous avez sélectionné.

Les paramètres du produit suivants s'appliquent lorsque Bitdefender fonctionne en Mode Batterie :

La Mise à jour Automatique de Bitdefender est reportée.

Les analyses planifiées sont reportées.

Le Widget Windows est désactivé.

Bitdefender détecte le passage d'une alimentation secteur à une alimentation sur batterie et, en fonction du niveau de charge de la batterie, passe automatiquement en Mode Batterie.De la même manière, Bitdefender quitte automatiquement le Mode Batterie lorsqu'il détecte que l'ordinateur portable ne fonctionne plus sur batterie.

Pour activer ou désactiver le mode Batterie, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Outils**.
3. Cliquez sur le module **Profils**.
4. Dans la fenêtre **Profils**, sélectionnez l'onglet **Mode Batterie**.
5. Activez ou désactivez le mode Batterie automatique en cliquant sur le bouton correspondant.

   Faites glisser le curseur correspondant le long de l'échelle pour déterminer quand le système doit passer en Mode Batterie. Le mode est activé par défaut lorsque le niveau de charge de batterie est inférieur à 30%.



Note

Le Mode Batterie est activé par défaut sur les ordinateurs portables et les tablettes.

Configurer le Mode Batterie

Pour configurer le mode Batterie, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Outils**.
3. Cliquez sur le module **Profils**.
4. Dans la fenêtre **Profils**, sélectionnez l'onglet **Mode Batterie**.
5. Cliquez sur **Configurer**.
6. Sélectionnez les réglages du système à appliquer en cochant les options suivantes :

   Optimiser les paramètres du produit pour le mode Batterie.

Reporter les tâches des programmes en arrière-plan et de maintenance.

Reporter les mises à jour automatiques de Windows.

Ajuster les paramètres du plan d'alimentation pour le mode Batterie.

Désactiver les appareils externes et les ports du réseau.

7. Cliquez sur **Enregistrer** pour sauvegarder les modifications et fermer la fenêtre.

4.6. Paramètres de Bitdefender de la protection par mot de passe

Si vous n'êtes pas le seul utilisateur avec des droits d'administrateur qui utilise cet ordinateur, il vous est recommandé de protéger vos paramètres de Bitdefender par un mot de passe.

Pour configurer la protection par mot de passe des paramètres de Bitdefender, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur l'icône en haut de la fenêtre et sélectionnez **Paramètres généraux** dans le menu déroulant.
3. Dans la fenêtre **Paramètres généraux**, sélectionnez l'onglet **Paramètres généraux**.
4. Activez la protection par mot de passe en cliquant sur le bouton.
5. Entrez le mot de passe dans les deux champs puis cliquez sur **OK**.(8 caractères minimum)

Une fois que vous avez défini un mot de passe, toute personne essayant de modifier les paramètres de Bitdefender devra indiquer ce mot de passe.



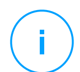
Important

N'oubliez pas votre mot de passe ou conservez-le en lieu sûr. Si vous oubliez le mot de passe, vous devrez réinstaller le programme ou contacter le support Bitdefender.

Pour supprimer la protection par mot de passe, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.

2. Cliquez sur l'icône en haut de la fenêtre et sélectionnez **Paramètres généraux** dans le menu déroulant.
3. Dans la fenêtre **Paramètres généraux**, sélectionnez l'onglet **Paramètres généraux**.
4. Désactivez la protection par mot de passe en cliquant sur le bouton. Entrez le mot de passe puis cliquez sur **OK**.



Note
Pour modifier le mot de passe de votre produit, cliquez sur le lien **Changer de mot de passe**.

4.7. Rapports d'utilisation anonymes

Par défaut, Bitdefender envoie des rapports contenant des informations sur votre utilisation aux serveurs Bitdefender.Ces informations sont essentielles pour améliorer le produit et nous aider à vous offrir un meilleur service à l'avenir. Veuillez noter que ces rapports ne comprendront aucune donnée confidentielle, telle que votre nom ou votre adresse IP, et ne seront pas utilisés à des fins commerciales.

Si vous souhaitez cesser d'envoyer des rapports d'utilisation anonymes, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur l'icône en haut de la fenêtre et sélectionnez **Paramètres généraux** dans le menu déroulant.
3. Dans la fenêtre **Paramètres généraux**, sélectionnez l'onglet **Avancé**.
4. Cliquez sur le bouton pour désactiver les rapports d'utilisation anonymes.

4.8. Offres spéciales et notifications du produit

Le produit Bitdefender est configuré pour vous signaler via une fenêtre pop-up les offres promotionnelles disponibles.Cela vous donne la possibilité de bénéficier de tarifs avantageux et de protéger vos appareils plus longtemps.

Des notifications du produit peuvent apparaître également lorsque des modifications sont effectuées par l'utilisateur dans le produit.

Pour activer ou désactiver les offres spéciales et les notifications du produit, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur l'icône en haut de la fenêtre et sélectionnez **Paramètres généraux** dans le menu déroulant.
3. Dans la fenêtre **Paramètres généraux**, sélectionnez l'onglet **Paramètres généraux**.
4. Activez ou désactivez les offres spéciales et les notifications du produit en cliquant sur le bouton correspondant.

L'option des offres spéciales et des notifications du produit est activée par défaut.



Note

Après avoir désactivé les offres spéciales et les notifications du produit, Bitdefender continuera à vous signaler les offres spéciales lorsque vous utiliserez une version d'évaluation, lorsque votre abonnement arrivera à expiration ou lorsque vous utiliserez une version du produit ayant expiré.

5. INTERFACE DE BITDEFENDER

Bitdefender Internet Security 2015 répond aux besoins de tous les utilisateurs, qu'ils soient débutants ou armés de solides connaissances techniques. Son interface utilisateur graphique est conçue pour s'adapter à chaque catégorie d'utilisateurs.

Pour afficher l'état du produit et effectuer des tâches essentielles, l'icône de la zone de notification de Bitdefender est disponible à tout moment.

La fenêtre principale vous donne accès à d'importantes informations sur le produit, aux modules du programme et vous permet d'effectuer des tâches courantes. La fenêtre principale vous permet d'accéder aux Panneaux pour une configuration détaillée et des tâches d'administration avancées, et de gérer le comportement du produit à l'aide d'Autopilot et des Profils.

Si vous souhaitez garder en permanence un œil sur les informations de sécurité essentielles et disposer d'un accès rapide aux principaux paramètres, ajoutez le Widget Window à votre bureau.

5.1. Icône de la zone de notification

Pour gérer l'ensemble du produit plus rapidement, vous pouvez utiliser l'icône Bitdefender de la zone de notification.



Note

Si vous utilisez Windows Vista, Windows 7, ou Windows 8, l'icône de Bitdefender ne sera peut-être pas visible en permanence. Pour que l'icône soit présente en permanence, procédez comme suit :

1. Cliquez sur la flèche dans l'angle inférieur droit de l'écran.
2. Cliquez sur **Personnaliser...** pour ouvrir la fenêtre Icônes de la Zone de Notification.
3. Sélectionnez l'option **Afficher les icônes et les notifications** pour l'icône **Agent Bitdefender**.

Double-cliquez sur cette icône pour ouvrir Bitdefender. Un clic droit sur l'icône donne également accès à un menu contextuel qui vous permettra de rapidement administrer le produit Bitdefender.



Icône

Afficher - ouvre la fenêtre principale de Bitdefender.

À propos de - Affichage d'une fenêtre contenant des informations relatives à Bitdefender, ainsi que des éléments d'aide si vous rencontrez une situation anormale.

Voir les problèmes de sécurité - vous aide à résoudre les problèmes de vulnérabilité en matière de sécurité.Si l'option n'est pas disponible, c'est qu'il n'y a pas de problème à corriger.Pour plus d'information, consultez *« Correction des problèmes »* (p. 13).

Afficher / Masquer le Widget Windows - permet d'activer / de désactiver le Widget Windows.

Mettre à jour - lance immédiatement une mise à jour.Vous pouvez suivre l'état de mise à jour dans le panneau Mise à jour de la fenêtre principale de Bitdefender.

Afficher le rapport de sécurité - ouvre une fenêtre où vous pouvez voir un rapport hebdomadaire et des recommandations pour votre système.Vous pouvez suivre les recommandations pour améliorer la sécurité de votre système.

L'icône de la zone de notification de Bitdefender vous informe de la présence de problèmes affectant la sécurité de votre ordinateur et du fonctionnement du programme en affichant un symbole spécial :

Des problèmes critiques affectent la sécurité de votre système. Ils requièrent votre attention immédiate et doivent être réglés dès que possible.
Des problèmes non critiques affectent la sécurité de votre système. Nous vous recommandons de les vérifier et de les corriger lorsque vous avez le temps.
L'Autopilot de Bitdefender est activé.

Si Bitdefender ne fonctionne pas, l'icône de la zone de notification apparaît sur un fond gris : .Cela se produit généralement lorsque la clé de licence est expirée. Cela peut également avoir lieu lorsque les services Bitdefender ne répondent pas ou lorsque d'autres erreurs affectent le fonctionnement normal de Bitdefender.

5.2. Fenêtre principale

La fenêtre principale de Bitdefender permet d'effectuer des tâches courantes, de corriger rapidement des problèmes de sécurité, d'afficher des informations sur le fonctionnement du produit et de configurer le produit. Tout se trouve à quelques clics.

La fenêtre est organisée en deux zones principales :

Barre d'outils supérieure
: Cette section vous permet de connaître l'état de sécurité de votre ordinateur, de configurer le comportement de Bitdefender dans certains cas et d'accéder à des tâches importantes.

Panneaux
: Vous pouvez gérer ici les principaux modules de Bitdefender et exécuter différentes tâches pour assurer la protection de votre système et son fonctionnement à une vitesse optimale.

L'icône en haut de la fenêtre vous permet de gérer votre compte et d'accéder aux fonctionnalités en ligne de votre produit depuis le tableau de bord du compte. Vous pouvez également accéder ici aux Événements, au Rapport de sécurité hebdomadaire et à la page Aide & Support.

Lier	Description
Nombre de jours restants	Le temps restant avant l'expiration de votre licence actuelle est indiqué.Cliquez sur le lien pour ouvrir une fenêtre dans laquelle vous pouvez voir plus d'informations sur votre clé de licence ou activer votre produit avec une nouvelle clé de licence.
Acheter	Vous aide à acheter une clé de licence pour votre produit Bitdefender Internet Security 2015.

5.2.1. Barre d'outils supérieure

La barre d'outils supérieure contient les éléments suivants :

La **Zone d'état de sécurité** à gauche de la barre d'outils vous indique si des problèmes affectent la sécurité de votre ordinateur et vous aide à les corriger.

La couleur de la zone d'état de la sécurité change en fonction des problèmes détectés et différents messages s'affichent :

La zone est en vert. Il n'y a pas de problèmes à corriger. Votre ordinateur et vos données sont protégés.

La zone est en jaune. Des problèmes non critiques affectent la sécurité de votre système. Nous vous recommandons de les vérifier et de les corriger lorsque vous avez le temps.

La zone est en rouge. Des problèmes critiques affectent la sécurité de votre système. Nous vous recommandons de vous occuper de ces problèmes immédiatement.

En cliquant sur la zone d'état de la sécurité, vous pouvez accéder à un assistant qui vous aidera à supprimer facilement toutes les menaces de votre ordinateur.Pour plus d'information, consultez « *Correction des problèmes* » (p. 13).

Autopilot vous permet de lancer l'Autopilot et de profiter d'une sécurité totalement silencieuse. Pour plus d'informations, consultez « *Autopilot* » (p. 17).

Les **Profils** vous permettent de travailler, de jouer ou de regarder des films et vous font gagner du temps en configurant le système afin qu'il remette à plus tard les tâches de maintenance. Pour plus d'informations, consultez « *Profils* » (p. 189).

5.2.2. Panneaux

Les panneaux sont constitués de deux parties, l'une à gauche de la fenêtre qui vous permet d'accéder et de gérer les modules de Bitdefender et l'autre à droite où vous pouvez lancer des tâches importantes à l'aide des boutons d'action.

Les panneaux disponibles dans cette zone sont :

Protection
Vie privée
Outils
Boutons d'action

Protection

Ce panneau vous permet de configurer votre niveau de sécurité, de gérer les amis et les spammeurs, d'afficher et d'éditer les paramètres de connexion du réseau et de configurer les vulnérabilités du système à corriger.

Les modules que vous pouvez gérer dans le panneau Protection sont les suivants :

Antivirus

La protection antivirus est la base de votre sécurité. Bitdefender vous protège en temps réel et à la demande contre toutes sortes de malwares tels que les virus, les chevaux de Troie, les spywares, les adwares etc.

Le module Antivirus vous permet d'accéder facilement aux tâches d'analyse suivantes :

- Analyse rapide
- Analyse du système
- Gestion des analyses
- Mode de secours

Pour plus d'informations sur les tâches d'analyse et sur comment configurer la protection antivirus, consultez *« Protection antivirus »* (p. 91).

Pare-feu

Le pare-feu vous protège lorsque vous êtes connecté à des réseaux et à Internet en filtrant toute tentative de connexion.

Pour plus d'informations sur la configuration du pare-feu, consultez *« Pare-feu »* (p. 139).

Détection d'Intrusion

La Détection d'Intrusion analyse les activités du système et du réseau à la recherche de comportements anormaux et d'attaques éventuelles.

Pour plus d'informations sur comment configurer la Détection d'Intrusion pour protéger les activités du système et du réseau, reportez-vous à *« Détection d'Intrusion »* (p. 148).

Protection Web

La protection web vous aide à être protégé contre les attaques de phishing, les tentatives de fraude et les fuites de données personnelles lorsque vous naviguez sur Internet.

Pour plus d'informations sur comment configurer Bitdefender pour protéger vos activités en ligne, reportez-vous à *« Protection Web »* (p. 127).

Antispam

Le module antispam Bitdefender protège votre boîte de réception contre les e-mails indésirables en filtrant le trafic de messagerie POP3.

Pour plus d'informations sur la protection antispam, reportez-vous à *« Antispam »* (p. 117).

Vulnérabilité

Le module Vulnérabilité vous aide à maintenir actualisés le système d'exploitation et les applications que vous utilisez régulièrement.

Cliquez sur **Analyse de Vulnérabilité** dans le module Vulnérabilité pour commencer à identifier les mises à jour critiques de Windows, les mises à jour d'applications et les mots de passe vulnérables appartenant à des comptes Windows.

Pour plus d'informations sur la configuration de la protection contre les vulnérabilités, reportez-vous à *« Vulnérabilité »* (p. 135).

Vie privée

Le panneau Vie privée vous permet de crypter vos données confidentielles, de protéger vos transactions en ligne, de sécuriser votre navigation sur Internet et de protéger vos enfants en vous offrant la possibilité de voir et de limiter leurs activités en ligne.

Les modules que vous pouvez gérer dans le panneau Vie privée sont les suivants :

Protection des données

Le module Protection des données empêche les fuites de données sensibles lorsque vous êtes en ligne et vous permet de supprimer des fichiers définitivement.
Cliquez sur **Destructeur de Fichiers** dans le module Protection des données pour lancer un assistant qui vous permettra de supprimer complètement des fichiers de votre système.

Pour plus d'informations sur la configuration de la protection des données, reportez-vous à *« Protection des données »* (p. 131).

Wallet

Wallet est le gestionnaire de mots de passe qui vous aide à conserver vos mots de passe, protège votre vie privée et vous offre une expérience de navigation sécurisée.

Le module Wallet vous permet de sélectionner les tâches suivantes :

Ouvrir Wallet - ouvre la base de données d'un Wallet existant.

Exporter Wallet - sauvegarde la base de données existante sur votre système.

Créer un Wallet - lance un assistant qui vous permet de créer une nouvelle base de données Wallet.

Pour plus d'informations sur la configuration de Wallet, reportez-vous à « *Protection Wallet de vos identifiants* » (p. 154).

Contrôle parental

Le Contrôle Parental de Bitdefender vous permet de surveiller ce que votre enfant fait sur l'ordinateur. En cas de contenu inapproprié vous pouvez décider de limiter son accès à Internet ou à certaines applications.

Cliquez sur **Configurer** dans le module du Contrôle parental afin de commencer à configurer les comptes Windows de vos enfants et ainsi suivre leurs activités en ligne.

Pour plus d'informations sur la configuration du contrôle parental, consultez « *Contrôle parental* » (p. 161).

Safepay

Le navigateur Bitdefender Safepay™ vous aide à assurer la confidentialité et la sécurité de vos transactions bancaires, de vos achats en ligne et de tout autre type de transaction sur Internet.

Cliquez sur **Ouvrir Safepay** dans le module Safepay pour commencer à effectuer des transactions en ligne dans un environnement sécurisé.

Pour plus d'informations sur Bitdefender Safepay™, reportez-vous à « *La sécurité Safepay pour les transactions en ligne* » (p. 149).

Outils

Le panneau Outils vous permet de configurer votre profil, d'améliorer la vitesse du système, de sauvegarder des fichiers importants et d'utiliser votre compte Facebook en toute sécurité.

Les modules que vous pouvez gérer dans le panneau Outils sont les suivants :

Safego

Bitdefender Safego est la solution de sécurité qui assure un environnement en ligne sûr aux utilisateurs de Facebook en surveillant à la fois leurs activités sur les réseaux sociaux et celles de leurs amis et en leur signalant tous les posts potentiellement malveillants.

Pour plus d'informations, consultez *« Protection Safego pour Facebook »* (p. 174).

Optimisation

Bitdefender Internet Security 2015 offre plus que de la sécurité, et contribue également aux bonnes performances de votre ordinateur.

Le module Optimisation vous permet d'accéder à des outils utiles :

Optimisation en 1 clic
Optimisation du démarrage
Nettoyage du PC
Défragmentation
Nettoyage du registre
Restauration du Registre
Détecteur de doublons

Pour plus d'informations sur les outils d'optimisation des performances, veuillez vous référer à *« Optimisation »* (p. 180).

Profils

Les Profils Bitdefender vous aident à profiter d'une expérience utilisateur simplifiée lorsque vous travaillez, regardez un film ou jouez en surveillant le logiciel et les outils de travail du système. Cliquez sur **Enregistrer** sur la barre d'outils supérieure dans l'interface de Bitdefender pour commencer à utiliser cette fonctionnalité.

Bitdefender vous permet de configurer les profils suivants :

Profil Travail
Profil Film
Profil Jeu

Pour plus d'informations sur comment configurer le module profils, reportez-vous à *« Profils »* (p. 189).

Boutons d'action

La section consacrée aux boutons d'action vous permet d'effectuer des tâches importantes liées à la sécurité de vos activités. Lorsque vous avez besoin d'exécuter une analyse, de mettre à jour le produit, de protéger vos transactions en ligne ou d'optimiser la vitesse de votre système, utilisez les options suivantes :

Analyse
Exécutez une analyse rapide pour vérifier qu'aucun virus n'est présent sur votre ordinateur.

Mise à jour
Mettez à jour votre Bitdefender pour vous assurer de disposer des dernières signatures de malwares.

Safepay
Ouvrez Safepay pour protéger vos données sensibles lorsque vous effectuez des transactions en ligne.

Optimisation
Libérez de l'espace sur le disque, corrigez les erreurs du registre et protégez votre vie privée en supprimant les fichiers qui ne sont plus utiles d'un simple clic sur un bouton.

5.3. Les modules Bitdefender

Le logiciel Bitdefender dispose d'un certain nombre de modules utiles qui vous aident notamment à travailler, à surfer sur Internet ou à effectuer des paiements en ligne en toute sécurité ainsi qu'à améliorer la rapidité de votre système. Lorsque vous souhaitez accéder à des modules ou commencer à configurer votre produit, cliquez sur les panneaux **Protection**, **Vie privée** et **Outils** dans l'interface de Bitdefender.

La liste suivante décrit brièvement chaque module.

Antivirus
Vous permet de configurer votre protection contre les malwares, de définir des exceptions d'analyse et de gérer les fichiers en quarantaine.

Antispam
Vous permet de conserver votre boîte de réception sans SPAM et de configurer les paramètres antispam en détail.

Protection Web
Vous permet de savoir si les informations des pages web que vous souhaitez consulter sont sûres.

Vulnérabilité
Vous permet de détecter et corriger les vulnérabilités de votre système.

Protection des données
Vous permet d'éviter les fuites de données et de protéger votre vie privée lorsque vous êtes en ligne.

Pare-feu
Vous permet de configurer les paramètres généraux du pare-feu et de gérer les règles.

Détection d'Intrusion
Vous permet de surveiller et d'analyser les activités du système et du réseau à la recherche de comportements anormaux et d'attaques éventuelles.

Wallet
Vous permet d'accéder à vos identifiants avec un mot de passe maître.

Profils
Vous permet de configurer votre profil actif pour une grande convivialité du système.

Contrôle parental
Vous permet de protéger vos enfants contre les contenus inappropriés en appliquant vos droits d'accès personnalisés à l'ordinateur.

Optimisation
Vous permet de surveiller les performances de votre ordinateur et de garder un œil sur la consommation de ressources.

5.4. Widget de sécurité

Le **Widget Windows** est une façon simple et rapide de surveiller et de contrôler Bitdefender Internet Security 2015. Ajouter ce petit widget discret à votre bureau vous permet de voir des informations critiques et d'effectuer des tâches essentielles à tout moment :

- ouvrir la fenêtre principale de Bitdefender.
- surveiller l'activité d'analyse en temps réel.
- surveiller l'état de sécurité de votre système et corriger tout problème existant.
- voir quand une mise à jour est en cours.
- afficher des notifications et accéder aux derniers événements signalés par Bitdefender.

analyser des fichiers ou des dossiers en glissant-déposant un ou plusieurs éléments sur le widget.



Widget de sécurité

L'état de sécurité global de votre ordinateur s'affiche **au centre** du widget. L'état est indiqué par la couleur et la forme de l'icône qui s'affiche dans cette zone.

Des problèmes critiques affectent la sécurité de votre système.

Ils requièrent votre attention immédiate et doivent être réglés dès que possible. Cliquez sur l'icône d'état pour commencer à corriger les problèmes signalés.

Des problèmes non critiques affectent la sécurité de votre système. Nous vous recommandons de les vérifier et de les corriger lorsque vous avez le temps. Cliquez sur l'icône d'état pour commencer à corriger les problèmes signalés.

Votre système est protégé.

Lorsqu'une tâche d'analyse à la demande est en cours, cette icône animée apparaît.

Lorsque des problèmes sont signalés, cliquez sur l'icône d'état pour lancer l'assistant de correction des problèmes.

La partie inférieure du widget affiche le compteur d'événements non lus (le nombre d'événements importants signalés par Bitdefender, s'il y en a). Cliquez sur le compteur d'événements, par exemple pour un événement non lu, pour ouvrir la fenêtre Événements. Pour plus d'informations, reportez-vous à « *Événements* » (p. 15).

5.4.1. Analyse des fichiers et des dossiers

Vous pouvez utiliser le Widget Windows pour analyser rapidement des fichiers et des dossiers. Faites glisser tout fichier ou dossier que vous souhaitez analyser et déposez-le sur le **Widget Windows**.

L'Assistant d'analyse antivirus s'affichera et vous guidera au cours du processus d'analyse.Les options d'analyse sont déjà configurées pour que la détection soit la meilleure possible et ne peuvent pas être modifiéesSi des fichiers infectés sont détectés, Bitdefender essaiera de les désinfecter (de supprimer les codes malveillants). Si la désinfection échoue, l'Assistant d'analyse antivirus vous proposera d'indiquer d'autres moyens d'intervenir sur les fichiers infectés.

5.4.2. Masquer / afficher le Widget Windows

Lorsque vous ne souhaitez plus voir le widget, cliquez sur ⊗.

Pour restaurer le Widget Windows, utilisez l'une des méthodes suivantes :

Dans la zone de notification :

1. Faites un clic droit sur l'icône de Bitdefender dans la zone de notification.
2. Cliquez sur **Afficher le Widget Windows** dans le menu contextuel qui apparaît.

À partir de l'interface de Bitdefender :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur l'icône en haut de la fenêtre et sélectionnez **Paramètres généraux** dans le menu déroulant.
3. Dans la fenêtre **Paramètres généraux**, sélectionnez l'onglet **Paramètres généraux**.
4. Activez **Afficher le Widget Windows** en cliquant sur le bouton correspondant.

5.5. Rapport de sécurité

Le rapport de sécurité fournit un rapport hebdomadaire pour votre produit et plusieurs conseils pour améliorer la protection du système. Ces conseils sont importants pour gérer la protection globale et vous pouvez voir facilement les actions que vous pouvez appliquer sur votre système.

Le rapport est généré une fois par semaine et résume les principales informations sur l'activité de votre produit afin que vous puissiez comprendre facilement ce qui s'est passé pendant cette période.

Les informations fournies par le rapport de sécurité sont divisées en deux catégories :

Zone **Protection** - permet d'afficher des informations liées à la protection de votre système.

Fichiers analysés

Vous permet de voir les fichiers analysés par Bitdefender pour la semaine. Vous pouvez afficher des informations comme le nombre de fichiers analysés et le nombre de fichiers nettoyés par Bitdefender.

Pour plus d'informations sur la protection antivirus, reportez-vous à « *Protection antivirus* » (p. 91).

Sites web analysés

Vous permet de consulter le nombre de pages web analysées et bloquées par Bitdefender. Pour vous protéger contre la divulgation d'informations personnelles lorsque vous êtes sur Internet, Bitdefender sécurise votre trafic web.

Pour plus d'informations sur la protection Web, reportez-vous à « *Protection Web* » (p. 127).

Vulnérabilités

Vous permet d'identifier et de corriger facilement les vulnérabilités du système afin de renforcer la protection de votre ordinateur contre les malwares et les pirates informatiques.

Pour plus d'informations sur l'analyse de vulnérabilité, consultez « *Vulnérabilité* » (p. 135).

Chronologie des événements

Vous permet d'avoir une image globale des processus d'analyse et des problèmes corrigés par Bitdefender au cours de la semaine. Les événements sont séparés par jours.

Pour plus d'informations sur un journal détaillé d'événements concernant l'activité sur votre ordinateur, consultez Événements.

La zone **Optimisation** - affiche des informations au sujet de l'espace libéré, des applications optimisées et de la quantité de batterie économisée avec le Mode Batterie.

Espace libéré

Vous permet de connaître la quantité d'espace libéré lors du processus d'optimisation du système. Bitdefender utilise l'Optimisation pour vous aider à améliorer la vitesse de votre système.

Pour plus d'informations sur l'Optimisation, reportez-vous à « *Optimisation* » (p. 180).

Batterie économisée

Vous permet de voir la quantité de batterie économisée lorsque le système fonctionnait en Mode Batterie.

Pour plus d'informations sur le Mode Batterie, reportez-vous à « *Mode Batterie* » (p. 19).

Applications optimisées

Vous permet de voir le nombre d'applications que vous avez utilisées sous les Profils.

Pour plus d'informations sur les Profils, reportez-vous à « *Profils* » (p. 189).

5.5.1. Consulter le rapport de sécurité

Le rapport de sécurité utilise un système de contrôle pour détecter la présence de problèmes pouvant affecter la sécurité de votre ordinateur et de vos données et vous en informer. Les problèmes détectés comprennent la désactivation d'importants paramètres de protection et d'autres conditions pouvant constituer un risque pour la sécurité. Utiliser le rapport vous permet de configurer des composants de Bitdefender spécifiques ou d'appliquer des actions préventives afin de protéger votre ordinateur et vos données confidentielles.

Pour consulter le rapport de sécurité, procédez comme suit :

1. Accédez au rapport :

   Ouvrez la fenêtre Bitdefender, cliquez sur l'icône en haut de la fenêtre puis sélectionnez **Rapport de sécurité** dans le menu déroulant.

Faites un clic droit sur l'icône de Bitdefender dans la zone de notification et sélectionnez **Afficher le rapport de sécurité**.

Lorsqu'un rapport est terminé, vous serez averti par une fenêtre contextuelle. Cliquez sur **Afficher** pour accéder au rapport de sécurité.

Une page Web s'ouvrira dans votre navigateur Web où vous pourrez voir le rapport généré.

2. Consultez la partie supérieure de la fenêtre pour voir l'état de sécurité global.
3. Consultez nos recommandations en bas de la page.

La couleur de la zone d'état de la sécurité change en fonction des problèmes détectés et différents messages s'affichent :

La zone est en vert. Il n'y a pas de problèmes à corriger. Votre ordinateur et vos données sont protégés.

La zone est en jaune. Des problèmes non critiques affectent la sécurité de votre système. Nous vous recommandons de les vérifier et de les corriger lorsque vous avez le temps.

La zone est en rouge. Des problèmes critiques affectent la sécurité de votre système. Nous vous recommandons de vous occuper de ces problèmes immédiatement.

5.5.2. Activer ou désactiver la notification Rapport de Sécurité

Pour activer ou désactiver la notification Rapport de sécurité, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur l'icône en haut de la fenêtre et sélectionnez **Paramètres généraux** dans le menu déroulant.
3. Dans la fenêtre **Paramètres généraux**, sélectionnez l'onglet **Paramètres généraux**.
4. Cliquez sur le bouton correspondant pour activer ou désactiver la notification Rapport de sécurité.

   La notification Rapport de sécurité est activée par défaut.

6. ACTIVER BITDEFENDER

Pour bénéficier de la protection de Bitdefender, vous devez activer votre logiciel avec une clé de licence.La clé de licence indique pendant combien de temps vous pouvez utiliser le produit.Dès que la clé de licence expire, Bitdefender cesse de réaliser ses fonctions et de protéger votre ordinateur.

Nous vous recommandons d'acheter une clé de licence ou de renouveler votre licence quelques jours avant l'expiration de la clé utilisée.Pour plus d'informations, consultez « *Acheter ou renouveler des clés de licence* » (p. 40).Si vous utilisez une version d'essai de Bitdefender, vous devez activer le produit avec une clé de licence si vous souhaitez continuer à l'utiliser après la fin de la période d'évaluation.

6.1. Saisie de votre clé de licence

Si vous avez choisi d'évaluer le produit lors de l'installation, vous pouvez l'utiliser pendant une période d'évaluation de 30 jours.Pour continuer à utiliser Bitdefender une fois la période d'essai terminée, vous devez activer le produit avec une clé de licence.

Un lien indiquant le nombre de jours restants à votre licence apparaît en bas de la fenêtre Bitdefender. Cliquez sur ce lien pour ouvrir la fenêtre d'enregistrement.

Vous pouvez visualiser l'état de votre enregistrement Bitdefender, votre clé d'activation actuelle ou voir dans combien de jours la licence arrivera à son terme.

Pour activer Bitdefender Internet Security 2015 :

1. Saisissez la clé de licence dans le champ correspondant.



Note

Vous trouverez votre clé d'activation :

- sur l'étiquette du CD.
- sur le certificat de licence.
- sur le courriel de confirmation d'achat en ligne.

Si vous n'avez pas de clé de licence Bitdefender, cliquez sur le lien de la fenêtre pour ouvrir une page web vous permettant d'en acheter une.

2. Cliquez sur **Activer**.

Même après avoir acheté une clé de licence, tant que l'enregistrement du produit avec la clé ne sera pas terminé, Bitdefender Internet Security 2015 continuera à apparaître comme une version d'évaluation.

6.2. Acheter ou renouveler des clés de licence

Si la période d'essai est sur le point d'expirer, vous devez acheter une clé de licence et activer votre produit.De même, si votre clé de licence actuelle est sur le point d'expirer, vous devez renouveler votre licence.

Bitdefender vous avertira à l'approche de la date d'expiration de votre licence. Suivez les instructions de l'alerte pour acheter une nouvelle licence.

Vous pouvez vous rendre sur une page web où vous pouvez acheter une clé de licence à tout moment, en procédant comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le lien indiquant le nombre de jours restants à votre licence, situé en bas de la fenêtre Bitdefender, pour ouvrir la fenêtre d'enregistrement du produit.
3. Cliquez sur **Vous n'avez pas de clé de licence ? Achetez-en une maintenant !**
4. Une page web s'ouvrira dans votre navigateur web, vous permettant d'acheter une clé de licence Bitdefender.

7. COMPTE MYBITDEFENDER

Les fonctionnalités en ligne de votre produit et les services supplémentaires de Bitdefender sont disponibles exclusivement via MyBitdefender. Vous devez lier votre ordinateur à MyBitdefender en vous connectant à un compte depuis Bitdefender Internet Security 2015 afin d'effectuer l'une des actions suivantes :

Récupérez votre clé de licence, si jamais vous la perdez.

Configurer les paramètres du Contrôle parental pour les comptes Windows de vos enfants et surveiller leurs activités où que vous soyez.

Protégez votre compte Facebook avec Safego.

Plusieurs solutions de sécurité Bitdefender pour PC et d'autres plateformes s'intègrent à MyBitdefender. Vous pouvez gérer la sécurité de tous les appareils liés à votre compte depuis un seul tableau de bord centralisé.

Votre compte MyBitdefender est accessible depuis tout appareil connecté à Internet sur https://my.bitdefender.com.

Vous pouvez également accéder à votre compte et le gérer directement depuis votre produit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur l'icône en haut de la fenêtre et sélectionnez **MyBitdefender** dans le menu déroulant.

7.1. Lier l'ordinateur à MyBitdefender

Pour lier votre ordinateur à un compte MyBitdefender, vous devez vous connecter à un compte depuis Bitdefender Internet Security 2015. Tant que votre ordinateur ne sera pas lié à MyBitdefender, vous devrez vous connecter à MyBitdefender à chaque fois que vous souhaitez utiliser une fonctionnalité nécessitant un compte.

Pour ouvrir la fenêtre MyBitdefender à partir de laquelle vous pouvez créer ou vous connecter à un compte, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur l'icône en haut de la fenêtre et sélectionnez **Compte** dans le menu déroulant.

Si vous êtes déjà connecté à un compte, le compte auquel vous êtes connecté s'affiche. Cliquez sur **Se connecter avec un autre compte** pour changer le compte lié à l'ordinateur.

Si vous êtes déjà connecté à un compte, le compte auquel vous êtes connecté s'affiche. Cliquez sur **Aller à MyBitdefender** pour aller dans votre tableau de bord. Pour changer le compte lié à l'ordinateur, cliquez sur **Se connecter avec un autre compte**.

Si vous ne vous êtes pas connecté à un compte, procédez en fonction de votre situation.

Je souhaite créer un compte MyBitdefender

Pour créer un compte MyBitdefender, suivez ces étapes :

1. Sélectionnez **Créer un nouveau compte**.

   Une nouvelle fenêtre s'affiche.

2. Tapez les informations requises dans les champs correspondants. Les informations fournies resteront confidentielles.

   Courriel - indiquez votre adresse courriel.

   Nom d'utilisateur - indiquez un nom d'utilisateur pour votre compte.

   Mot de passe - saisissez un mot de passe pour votre compte.Le mot de passe doit contenir au moins 6 caractères.

   Confirmer le mot de passe - saisissez à nouveau votre mot de passe.

3. Cliquez sur **Créer**.

4. Vous devez terminer l'enregistrement de votre compte avant de pouvoir l'utiliser. Consultez votre messagerie et suivez les instructions de l'e-mail de confirmation envoyé par Bitdefender.

Je souhaite me connecter à l'aide de mon compte Microsoft, Facebook ou Google

Pour vous connecter avec votre compte Microsoft, Facebook ou Google, procédez comme suit :

1. Cliquez sur l'icône du service que vous souhaitez utiliser pour vous connecter. Vous serez redirigé vers la page de connexion de ce service.

2. Suivez les instructions du service sélectionné pour lier votre compte à Bitdefender.



Note
Bitdefender n'accède à aucune information confidentielle telle que le mot de passe du compte que vous utilisez pour vous connecter, ou les informations personnelles de vos amis et contacts.

J'ai déjà un compte MyBitdefender

Si vous avez déjà un compte mais ne vous y êtes pas encore connecté, suivez les étapes suivantes pour vous y connecter :

1. Tapez l'adresse courriel et le mot de passe de votre compte dans les champs correspondants.



Note
Si vous avez oublié votre mot de passe, cliquez sur **Mot de passe oublié** et suivez les instructions pour le retrouver.

2. Cliquez sur **Se connecter à MyBitdefender**.

Une fois l'ordinateur lié à un compte, vous pouvez utiliser l'adresse courriel et le mot de passe fournis pour vous connecter à https://my.bitdefender.com.

Vous pouvez également accéder à votre compte directement à partir de Bitdefender Internet Security 2015 en cliquant sur l'icône en haut de la fenêtre et en sélectionnant **MyBitdefender** dans le menu déroulant.

8. MAINTENIR BITDEFENDER À JOUR

De nouveaux virus sont trouvés et identifiés chaque jour. C'est pourquoi il est très important que Bitdefender soit à jour dans les signatures de codes malveillants.

Si vous êtes connecté à Internet par câble ou DSL, Bitdefender s'en occupera automatiquement. Par défaut, des mises à jour sont recherchées au démarrage de votre ordinateur puis toutes les **heures** par la suite.Si une mise à jour est détectée, elle est automatiquement téléchargée et installée sur votre ordinateur.

Le processus de mise à jour est exécuté à la volée, ce qui signifie que les fichiers nécessitant une mise à jour sont remplacés progressivement. Ainsi, le processus de mise à jour n'affecte pas le fonctionnement du produit tout en excluant tout problème de vulnérabilité en matière de sécurité.



Important

Pour être protégé contre les dernières menaces, maintenez la mise à jour automatique activée.

Votre intervention peut être nécessaire, dans certains cas, pour maintenir la protection de Bitdefender à jour :

Si votre ordinateur se connecte à Internet via un serveur proxy, vous devez configurer les paramètres du proxy comme indiqué dans *« Comment configurer Bitdefender pour utiliser une connexion Internet par proxy ? »* (p. 83).

Si vous n'avez pas de connexion Internet, vous pouvez mettre à jour Bitdefender manuellement comme indiqué dans *« Mon ordinateur n'est pas connecté à Internet. Comment actualiser Bitdefender? »* (p. 207).Le fichier de mise à jour manuelle est publié une fois par semaine.

Des erreurs peuvent se produire lors du téléchargement de mises à jour avec une connexion à Internet lente. Pour savoir comment éviter ces erreurs, veuillez consulter *« Comment mettre à jour Bitdefender avec une connexion Internet lente »* (p. 207).

Si vous êtes connecté à Internet via une connexion RTC (ou RNIS), nous vous conseillons de prendre l'habitude d'utiliser régulièrement les mises à jour à la demande de Bitdefender.Pour plus d'informations, consultez *« Mise à jour en cours »* (p. 45).

8.1. Vérifier que Bitdefender est à jour

Pour vérifier que la protection de Bitdefender est à jour, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Sur la **Zone d'état de sécurité**, à gauche de la barre d'outils, regardez quand a eu lieu la dernière mise à jour.

Pour des informations détaillées sur les dernières mises à jour, vérifiez les événements de mise à jour :

1. Dans la fenêtre principale, cliquez sur l'icône en haut de la fenêtre et sélectionnez **Événements** dans le menu déroulant.
2. Dans la fenêtre **Événements**, sélectionnez **Mise à jour** dans le menu déroulant correspondant.

Vous pouvez savoir quand des mises à jour ont été lancées et obtenir des informations à leur sujet (si elles ont été ou non réussies, si elles nécessitent un redémarrage pour que leur installation se termine).Si nécessaire, redémarrez le système dès que possible.

8.2. Mise à jour en cours

Pour effectuer des mises à jour, une connexion à Internet est requise.

Pour lancer une mise à jour, choisissez l'une des options suivantes :

Ouvrez la fenêtre Bitdefender et cliquez sur le bouton d'action **Mise à jour** à droite de la fenêtre.

Faites un clic droit sur l'icône de Bitdefender de la zone de notification et sélectionnez **Mettre à jour maintenant**.

Le module de mise à jour se connectera au serveur de mise à jour de Bitdefender et recherchera des mises à jour. Si une mise à jour est détectée, elle sera installée automatiquement ou il vous sera demandé de confirmer son installation, selon les paramètres de mise à jour.



Important

Il peut être nécessaire de redémarrer votre PC lorsque vous avez terminé une mise à jour. Il est recommandé de le faire dès que possible

8.3. Activer ou désactiver la mise à jour automatique

Pour activer ou désactiver la mise à jour automatique, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur l'icône en haut de la fenêtre et sélectionnez **Paramètres généraux** dans le menu déroulant.
3. Dans la fenêtre **Paramètres généraux**, sélectionnez l'onglet **Mise à jour**.
4. Cliquez sur le bouton pour activer ou désactiver la mise à jour automatique.
5. Une fenêtre d'avertissement s'affiche.Vous devez confirmer votre choix en sélectionnant dans le menu pour combien de temps vous souhaitez désactivez la mise à jour automatique. Vous pouvez désactiver la mise à jour automatique pendant 5, 15 ou 30 minutes, 1 heure, en permanence ou jusqu'au redémarrage du système.



Avertissement

Cela peut poser un problème de sécurité important. Nous vous recommandons de désactiver la mise à jour automatique pendant le moins de temps possible. Si Bitdefender n'est pas régulièrement mis à jour, il ne pourra pas vous protéger contre les dernières menaces.

8.4. Réglage des paramètres de mise à jour

Les mises à jour peuvent être réalisées depuis le réseau local, depuis Internet, directement ou à travers un serveur proxy.Par défaut, Bitdefender recherche les mises à jour chaque heure sur Internet et installe celles qui sont disponibles sans vous en avertir.

Les paramètres de mise à jour par défaut sont adaptés à la plupart des utilisateurs et vous n'avez normalement pas besoin de les modifier.

Pour régler les paramètres de mise à jour, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur l'icône en haut de la fenêtre et sélectionnez **Paramètres généraux** dans le menu déroulant.
3. Dans la fenêtre **Paramètres généraux**, sélectionnez l'onglet **Mise à jour** et ajustez les paramètres en fonction de vos préférences.

Emplacement de mise à jour

Bitdefender est configuré pour se mettre à jour à partir des serveurs de mise à jour de Bitdefender sur Internet. L'emplacement de mise à jour est une adresse Internet générique qui est automatiquement redirigée vers le serveur de mise à jour Bitdefender le plus proche de votre région.

Ne modifiez pas l'emplacement de mise à jour sauf sur demande d'un représentant de Bitdefender ou de votre administrateur réseau (si vous êtes connecté à un réseau d'entreprise).

Vous pouvez revenir à l'emplacement de mise à jour Internet générique en cliquant sur **Par défaut**.

Règles de traitement

Vous disposez de trois façons de télécharger et d'installer des mises à jour :

Mise à jour silencieuse - Bitdefender télécharge et implémente automatiquement la mise à jour.

Demander avant de télécharger les mises à jour - à chaque fois qu'une mise à jour sera disponible, le système demandera votre autorisation avant de la télécharger.

Demander avant l'installation - à chaque fois qu'une mise à jour est téléchargée, le système demande votre autorisation avant de l'installer.

Certaines mises à jour nécessitent un redémarrage pour terminer l'installation. Par défaut, si une mise à jour nécessite un redémarrage, Bitdefender continuera à fonctionner avec les anciens fichiers jusqu'à ce que l'utilisateur redémarre volontairement l'ordinateur. Cela évite que le processus de mise à jour de Bitdefender interfère avec le travail de l'utilisateur.

Si vous souhaitez être averti lorsqu'une mise à jour nécessite un redémarrage, désactivez l'option **Reporter le redémarrage** en cliquant sur le bouton correspondant.

COMMENT FAIRE POUR

9. INSTALLATION

9.1. Comment installer Bitdefender sur un deuxième ordinateur ?

Si vous avez acheté une clé de licence pour plusieurs ordinateurs, vous pouvez utiliser la même clé de licence pour enregistrer un deuxième PC.

Pour installer Bitdefender correctement sur un second ordinateur, suivez les étapes suivantes :

1. Installez Bitdefender à partir du CD/DVD ou à l'aide du programme d'installation fourni dans l'e-mail d'achat en ligne et suivez les mêmes étapes d'installation.

   Au début de l'installation vous serez invité à télécharger les derniers fichiers d'installation disponibles.

2. Lorsque la fenêtre d'enregistrement apparaît, saisissez la clé de licence et cliquez sur **S'enregistrer**.

3. À l'étape suivante, vous avez la possibilité de vous connecter à votre compte MyBitdefender ou de créer un nouveau compte MyBitdefender.

   Vous pouvez également choisir de créer un compte MyBitdefender ultérieurement.

4. Attendez la fin du processus d'installation et fermez la fenêtre.

9.2. Quand devrais-je réinstaller Bitdefender ?

Dans certains cas, vous pouvez avoir besoin de réinstaller votre produit Bitdefender.

Quelques situations typiques nécessitant de réinstaller Bitdefender :

- vous avez réinstallé le système d'exploitation.
- vous avez acheté un nouvel ordinateur.
- vous souhaitez modifier la langue d'affichage de l'interface de Bitdefender .

Pour réinstaller Bitdefender, vous pouvez utiliser le disque d'installation que vous avez acheté ou télécharger une nouvelle version sur le site web de Bitdefender.

Au cours de l'installation, on vous demandera d'enregistrer le produit avec votre clé de licence.

Si vous perdez votre clé de licence, vous pouvez la retrouver en vous connectant à https://my.bitdefender.com. Tapez l'adresse courriel et le mot de passe de votre compte dans les champs correspondants.

Pour plus d'informations sur le processus d'installation de Bitdefender, reportez-vous à « *Installer Bitdefender* » (p. 5).

9.3. Où est-ce que je peux télécharger mon produit Bitdefender ?

Vous pouvez télécharger votre produit Bitdefender sur nos sites Web autorisés (par exemple, le site Web d'un partenaire de Bitdefender ou une boutique en ligne) ou sur notre site Web à l'adresse suivante : http://www.bitdefender.fr/Downloads/.



Note
Avant de lancer le kit, nous vous recommandons de désinstaller toutes les solutions antivirus présentes sur votre système. Lorsque vous utilisez plusieurs solutions de sécurité sur le même ordinateur, le système devient instable.

Pour installer Bitdefender, procédez comme suit :

1. Faites un double clic sur le programme d'installation que vous avez téléchargé et suivez les étapes d'installation.
2. Lorsque la fenêtre d'enregistrement apparaît, saisissez la clé de licence et cliquez sur **S'enregistrer**.
3. À l'étape suivante, vous avez la possibilité de vous connecter à votre compte MyBitdefender ou de créer un nouveau compte MyBitdefender.

   Vous pouvez également choisir de créer un compte MyBitdefender ultérieurement.
4. Attendez la fin du processus d'installation et fermez la fenêtre.

9.4. Comment passer d'un produit Bitdefender à un autre ?

Vous pouvez facilement passer d'un produit Bitdefender à un autre.

Les trois produits Bitdefender que vous pouvez installer sur votre système sont les suivants :

Bitdefender Antivirus Plus 2015

Bitdefender Internet Security 2015

Bitdefender Total Security 2015

Si vous n'avez pas de clé de licence pour le produit que vous souhaitez utiliser, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Pour accéder à la fenêtre d'enregistrement du produit, cliquez sur le lien qui indique le nombre de jours restants à votre licence, situé en bas de la fenêtre Bitdefender.
3. Cliquez sur **Vous n'avez pas de clé de licence ? Achetez-en une maintenant !**
4. Une page web s'ouvrira dans votre navigateur web, vous permettant d'acheter une clé de licence Bitdefender.

Une fois que vous avez acheté la clé de licence du produit Bitdefender que vous souhaitez utiliser, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Un lien indiquant le nombre de jours restants à votre licence apparaît en bas de la fenêtre Bitdefender.

   Cliquez sur ce lien pour ouvrir la fenêtre d'enregistrement.
3. Saisissez la clé de licence, puis cliquez sur **Enregistrer**.
4. Vous serez informé que la clé de licence correspond à un produit Bitdefender différent.

   Cliquez sur le lien correspondant et suivez la procédure pour effectuer l'installation.

9.5. Comment utiliser ma clé de licence Bitdefender après une mise à niveau Windows ?

Cette situation se produit lorsque vous mettez à niveau votre système d'exploitation et souhaitez continuer à utiliser votre clé de licence Bitdefender.

Si vous utilisez une version antérieure de Bitdefender vous pouvez la mettre à niveau, gratuitement, vers la dernière version de Bitdefender en procédant comme suit :

D'une ancienne version de Bitdefender Antivirus vers la dernière version de Bitdefender Antivirus disponible.

D'une ancienne version de Bitdefender Internet Security vers la dernière version de Bitdefender Internet Security disponible.

D'une ancienne version de Bitdefender Total Security vers la dernière version de Bitdefender Total Security disponible.

Deux situations peuvent se produire :

Vous avez mis à niveau le système d'exploitation à l'aide de Windows Update et vous remarquez que Bitdefender ne fonctionne plus.

Dans ce cas, vous avez besoin de réinstaller le produit avec la dernière version disponible.

Pour résoudre cette situation, suivez ces étapes :

1. Supprimez Bitdefender en procédant comme suit :

   Dans **Windows XP**:

   a. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Ajout/Suppression de programmes**.

   b. Localisez **Bitdefender Internet Security 2015** et sélectionnez **Supprimer**.

   c. Cliquez sur **Supprimer** dans la fenêtre qui apparaît puis sélectionnez **Je souhaite le réinstaller**.

   d. Attendez la fin du processus de désinstallation et puis redémarrez votre système.

   Dans **Windows Vista** et **Windows 7**:

   a. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.

   b. Localisez **Bitdefender Internet Security 2015** et sélectionnez **Désinstaller**.

   c. Cliquez sur **Supprimer** dans la fenêtre qui apparaît puis sélectionnez **Je souhaite le réinstaller**.

d. Attendez la fin du processus de désinstallation et puis redémarrez votre système.

Dans **Windows 8** :

a. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.

b. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.

c. Localisez **Bitdefender Internet Security 2015** et sélectionnez **Désinstaller**.

d. Cliquez sur **Supprimer** dans la fenêtre qui apparaît puis sélectionnez **Je souhaite le réinstaller**.

e. Attendez la fin du processus de désinstallation et puis redémarrez votre système.

2. Téléchargez le fichier d'installation en sélectionnant le produit pour lequel vous disposez d'une clé de licence valide.

   Vous pouvez télécharger le fichier d'installation sur le site Internet de Bitdefender à l'adresse suivante : http://www.bitdefender.fr/Downloads/.

3. Sélectionnez sur l'installer pour lancer le processus d'installation.

4. Lorsque la fenêtre d'enregistrement apparaît, saisissez la clé de licence et cliquez sur **S'enregistrer**.

5. À l'étape suivante, vous avez la possibilité de vous connecter à votre compte **MyBitdefender** ou de créer un nouveau compte **MyBitdefender**.

   Vous pouvez également choisir de créer un compte **MyBitdefender** ultérieurement.

   Attendez la fin du processus d'installation et fermez la fenêtre.

Vous avez changé de système et souhaitez continuer à utiliser la protection Bitdefender.

Vous avez donc besoin de réinstaller le produit avec la dernière version.

Pour résoudre cette situation, suivez ces étapes :

1. Téléchargez le fichier d'installation en sélectionnant le produit pour lequel vous disposez d'une clé de licence valide.

Vous pouvez télécharger le fichier d'installation sur le site Internet de Bitdefender à l'adresse suivante : http://www.bitdefender.fr/Downloads/.

2. Sélectionnez sur l'installer pour lancer le processus d'installation.
3. Lorsque la fenêtre d'enregistrement apparaît, saisissez la clé de licence et cliquez sur **S'enregistrer**.
4. À l'étape suivante, vous avez la possibilité de vous connecter à votre compte **MyBitdefender** ou de créer un nouveau compte **MyBitdefender**.

   Vous pouvez également choisir de créer un compte **MyBitdefender** ultérieurement.

   Attendez la fin du processus d'installation et fermez la fenêtre.

Pour plus d'informations sur le processus d'installation de Bitdefender, reportez-vous à « *Installer Bitdefender* » (p. 5).

9.6. Comment réparer Bitdefender ?

Si vous souhaitez réparer votre produit Bitdefender Internet Security 2015 à partir du menu Démarrer de Windows, procédez comme suit :

Dans **Windows XP**, **Windows Vista** et **Windows 7**:

1. Cliquez sur **Démarrer** et allez dans **Programmes**.
2. Localisez **Bitdefender Internet Security 2015** et sélectionnez **Désinstaller**.
3. Cliquez sur **Réparer** dans la fenêtre qui s'affiche.

   Cela prendra quelques minutes.
4. Vous aurez besoin de redémarrer l'ordinateur pour terminer le processus.

Dans **Windows 8** :

1. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
2. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.
3. Localisez **Bitdefender Internet Security 2015** et sélectionnez **Désinstaller**.
4. Cliquez sur **Réparer** dans la fenêtre qui s'affiche.

Cela prendra quelques minutes.

5. Vous aurez besoin de redémarrer l'ordinateur pour terminer le processus.

10. ACTIVATION

10.1. Quel est le produit Bitdefender que j'utilise ?

Pour découvrir quel programme Bitdefender vous avez installé, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. En haut de la fenêtre devrait apparaître l'un des éléments suivants :

   Bitdefender Antivirus Plus 2015

   Bitdefender Internet Security 2015

   Bitdefender Total Security 2015

10.2. Comment enregistrer une version d'essai ?

Si vous avez installé une version d'essai, vous ne pourrez l'utiliser que pendant une période limitée. Pour continuer à utiliser Bitdefender une fois la période d'essai terminée, vous devez enregistrer votre produit avec une clé de licence.

Pour enregistrer Bitdefender, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Un lien indiquant le nombre de jours restants à votre licence apparaît en bas de la fenêtre Bitdefender.

   Cliquez sur ce lien pour ouvrir la fenêtre d'enregistrement.
3. Saisissez la clé de licence, puis cliquez sur **S'enregistrer**.

   Si vous n'avez pas de clé de licence, cliquez sur le lien de la fenêtre pour vous rendre sur une page web vous permettant d'en acheter une.
4. Attendez la fin du processus d'enregistrement et fermez la fenêtre.

10.3. Quand ma protection Bitdefender expire-t-elle ?

Pour connaître le nombre de jours restants de votre clé de licence, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.

2. Un lien indiquant le nombre de jours restants à votre licence apparaît en bas de la fenêtre Bitdefender.
3. Pour des informations supplémentaires, cliquez sur le lien pour ouvrir la fenêtre d'enregistrement.
4. Dans la fenêtre **Enregistrement de votre produit**, vous pouvez :

   Voir la clé de licence actuelle

   Enregistrer avec une autre clé de licence

   Acheter une clé de licence

10.4. Comment renouveler ma protection Bitdefender ?

Lorsque votre protection Bitdefender est sur le point d'expirer, vous devez renouveler votre clé de licence.

Suivez ces étapes pour visiter un site web où vous pouvez renouveler votre clé de licence Bitdefender :

1. Ouvrez la fenêtre de Bitdefender.
2. Un lien indiquant le nombre de jours restants à votre licence apparaît en bas de la fenêtre Bitdefender. Cliquez sur ce lien pour ouvrir la fenêtre d'enregistrement.
3. Cliquez sur **Vous n'avez pas de clé de licence ? Achetez-en une maintenant !**
4. Une page web s'ouvrira dans votre navigateur web, vous permettant d'acheter une clé de licence Bitdefender.



Note
Vous pouvez également contacter le revendeur vous ayant vendu votre produit Bitdefender.

Suivez ces étapes pour enregistrer votre Bitdefender avec la nouvelle clé de licence :

1. Ouvrez la fenêtre de Bitdefender.

2. Un lien indiquant le nombre de jours restants à votre licence apparaît en bas de la fenêtre Bitdefender. Cliquez sur ce lien pour ouvrir la fenêtre d'enregistrement.
3. Saisissez la clé de licence, puis cliquez sur **S'enregistrer**.
4. Attendez la fin du processus d'enregistrement et fermez la fenêtre.

Pour plus d'informations, vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Demander de l'aide* » (p. 233).

11. MYBITDEFENDER

11.1. Comment me connecter à MyBitdefender à l'aide d'un autre compte en ligne ?

Vous avez créé un nouveau compte MyBitdefender et souhaitez l'utiliser à partir de maintenant.

Pour créer un autre compte, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur l'icône en haut de la fenêtre et sélectionnez **Compte** dans le menu déroulant.

   Si vous êtes déjà connecté à un compte, le compte auquel vous êtes connecté s'affiche. Cliquez sur **Se connecter avec un autre compte** pour changer le compte lié à l'ordinateur.

   Une nouvelle fenêtre s'affiche.
3. Tapez l'adresse courriel et le mot de passe de votre compte dans les champs correspondants.
4. Cliquez sur **Se connecter à MyBitdefender**

11.2. Comment changer l'adresse courriel utilisée pour le compte MyBitdefender ?

Vous avez créé un compte MyBitdefender avec une adresse courriel que vous n'utilisez plus et vous aimeriez la changer.

L'adresse courriel ne peut pas être modifiée mais vous pouvez utiliser une adresse courriel différente pour créer un nouveau compte en ligne.

Pour créer un autre compte MyBitdefender, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur l'icône en haut de la fenêtre et sélectionnez **Compte** dans le menu déroulant.

   Si vous êtes déjà connecté à un compte, le compte auquel vous êtes connecté s'affiche. Cliquez sur **Se connecter avec un autre compte** pour changer le compte lié à l'ordinateur.

Une nouvelle fenêtre s'affiche.

3. Sélectionnez **Créer un nouveau compte**.
4. Saisissez les informations requises dans les champs correspondants. Les informations fournies resteront confidentielles.

   Courriel - indiquez votre adresse courriel.

   Nom d'utilisateur - indiquez un nom d'utilisateur pour votre compte.

   Mot de passe - saisissez un mot de passe pour votre compte. Le mot de passe doit contenir au moins 6 caractères.

   Confirmer le mot de passe - saisissez à nouveau votre mot de passe.

   Cliquez sur **Créer**.
5. Vous devez terminer l'enregistrement de votre compte avant de pouvoir l'utiliser. Consultez votre messagerie et suivez les instructions de l'e-mail de confirmation envoyé par Bitdefender.

Saisissez la nouvelle adresse courriel pour vous connecter à MyBitdefender.

11.3. Comment redéfinir le mot de passe du compte MyBitdefender ?

Pour définir un nouveau mot de passe pour votre compte MyBitdefender, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur l'icône en haut de la fenêtre et sélectionnez **Compte** dans le menu déroulant.

   Une nouvelle fenêtre s'affiche.
3. Cliquez sur le lien **J'ai oublié mon mot de passe**.
4. Saisissez l'adresse courriel utilisée pour créer votre compte MyBitdefender et cliquez sur le lien **Récupérer le mot de passe**.
5. Consultez votre courriel et cliquez sur le lien indiqué.

   Une nouvelle fenêtre s'affiche.
6. Saisissez le nouveau mot de passe. Le mot de passe doit contenir au moins 6 caractères.

7. Saisissez de nouveau le mot de passe dans le champ **Retaper mot de passe**.
8. Cliquez sur **Envoyer**.

Pour accéder à votre compte MyBitdefender, saisissez votre adresse courriel et le nouveau mot de passe que vous venez de définir.

12. ANALYSER AVEC BITDEFENDER

12.1. Comment analyser un fichier ou un dossier ?

La méthode la plus simple pour analyser un fichier ou un dossier consiste à faire un clic droit sur l'objet que vous souhaitez analyser, à pointer sur Bitdefender et à sélectionner **Analyser avec Bitdefender** dans le menu.

Pour terminer l'analyse, suivez l'assistant d'analyse antivirus. Bitdefender appliquera automatiquement les actions recommandées aux fichiers détectés.

Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer.

Cette méthode d'analyse est à utiliser dans des situations courantes qui englobent les cas suivants :

- Vous soupçonnez un fichier ou un dossier donné d'être infecté.
- Quand vous téléchargez sur Internet des fichiers dont vous pensez qu'ils pourraient être dangereux.
- Analysez un dossier partagé sur le réseau avant de copier des fichiers sur votre ordinateur.

12.2. Comment analyser mon système ?

Pour effectuer une analyse complète du système, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Sous le module **Antivirus**, sélectionnez **Analyse du Système**.
4. Suivez les indications de l'assistant de l'analyse antivirus pour effectuer l'analyse. Bitdefender appliquera automatiquement les actions recommandées aux fichiers détectés.

   Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer. Pour plus d'informations, consultez *« Assistant d'analyse antivirus »* (p. 103).

12.3. Comment créer une tâche d'analyse personnalisée ?

Si vous souhaitez analyser certains emplacements de votre ordinateur ou configurer les options d'analyse, configurez et exécutez une analyse personnalisée.

Pour créer une tâche d'analyse personnalisée, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Sous le module **Antivirus**, sélectionnez **Gestion des analyses**.
4. Cliquez sur **Nouvelle tâche personnalisée** pour créer une nouvelle tâche d'analyse, et sélectionnez un emplacement à analyser.
5. Si vous souhaitez configurer les options d'analyse en détail, sélectionnez l'onglet **Avancé**.

   Vous pouvez facilement configurer les options d'analyse en réglant le niveau d'analyse. Déplacez le curseur sur l'échelle pour choisir le niveau d'analyse souhaité.

   Vous pouvez également choisir d'éteindre l'ordinateur une fois l'analyse terminée si aucune menace n'est détectée. N'oubliez pas qu'il s'agira du comportement par défaut à chaque fois que vous exécuterez cette tâche.
6. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.
7. Cliquez sur **Planifier** si vous souhaitez définir une planification pour cette tâche d'analyse.
8. Cliquez sur **Démarrer l'analyse** et suivez l'Assistant d'analyse antivirus pour terminer l'analyse. À la fin de l'analyse, on vous demandera de sélectionner les actions à appliquer aux fichiers détectés, le cas échéant.
9. Si vous le souhaitez, vous pouvez relancer rapidement une analyse personnalisée en cliquant sur le bouton correspondant dans la liste.

12.4. Comment exclure un dossier de l'analyse ?

Bitdefender vous permet d'exclure de l'analyse certains fichiers, dossiers ou extensions de fichiers.

Les exclusions doivent être employées par des utilisateurs ayant un niveau avancé en informatique et uniquement dans les situations suivantes :

Vous avez un dossier important sur votre système où se trouvent des films et de la musique.

Vous avez une archive importante sur votre système où se trouvent différentes données.

Vous gardez un dossier où vous installez différents types de logiciels et applications à des fins de test. L'analyse du dossier peut conduire à la perte de certaines données.

Pour ajouter le dossier à la liste d'exceptions, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Antivirus**.
4. Dans la fenêtre **Antivirus**, sélectionnez l'onglet **Exclusions**.
5. Veillez à ce qu'**Exclusions pour les fichiers** soit activé en cliquant sur le bouton.
6. Cliquez sur le lien **Fichiers et dossiers exclus**.
7. Cliquez sur le bouton **Ajouter**, situé en haut du tableau des exclusions.
8. Cliquez sur **Parcourir**, sélectionnez le dossier à exclure de l'analyse, puis cliquez sur **OK**.
9. Cliquez sur **Ajouter** puis sur **OK** pour sauvegarder les modifications et fermer la fenêtre.

12.5. Que faire lorsque Bitdefender a détecté un fichier sain comme étant infecté ?

Il arrive parfois que Bitdefender indique par erreur qu'un fichier légitime est une menace (une fausse alerte). Pour corriger cette erreur, ajoutez le fichier à la zone des exclusions de Bitdefender :

1. Désactivez la protection antivirus en temps réel de Bitdefender :
   a. Ouvrez la fenêtre de Bitdefender.
   b. Accédez au panneau **Protection**.

c. Cliquez sur le module **Antivirus**.

d. Dans la fenêtre **Antivirus**, sélectionnez l'onglet **Résident**.

e. Cliquez sur le bouton pour désactiver l'**Analyse à l'accès**.

Une fenêtre d'avertissement s'affiche. Vous devez confirmer votre choix en sélectionnant dans le menu pour combien de temps vous souhaitez désactivez la protection en temps- réel. Vous pouvez désactiver la protection en temps réel pendant 5, 15 ou 30 minutes, 1 heure, en permanence ou jusqu'au redémarrage du système.

2. Afficher les objets masqués dans Windows. Pour savoir comment faire cela, consultez *« Comment afficher des objets cachés dans Windows ? »* (p. 85).
3. Restaurer le fichier à partir de la zone de quarantaine :

a. Ouvrez la fenêtre de Bitdefender.

b. Accédez au panneau **Protection**.

c. Cliquez sur le module **Antivirus**.

d. Dans la fenêtre **Antivirus**, sélectionnez l'onglet **Quarantaine**.

e. Sélectionnez le fichier et cliquez sur **Restaurer**.

4. Ajouter le fichier à la liste d'exceptions. Pour savoir comment faire cela, consultez *« Comment exclure un dossier de l'analyse ? »* (p. 63).
5. Activez la protection antivirus en temps réel de Bitdefender.
6. Contactez les représentants de notre soutien technique afin que nous puissions supprimer la signature de détection. Pour savoir comment faire cela, consultez *« Demander de l'aide »* (p. 233).

12.6. Comment connaître les virus détectés par Bitdefender ?

À chaque fois qu'une analyse est effectuée, un journal d'analyse est créé et Bitdefender enregistre les problèmes détectés.

Le rapport d'analyse contient des informations détaillées sur le processus d'analyse, telles que les options d'analyse, la cible de l'analyse, les menaces trouvées et les actions prises à l'encontre de ces menaces.

Vous pouvez ouvrir le journal d'analyse directement à partir de l'assistant d'analyse, une fois l'analyse terminée, en cliquant sur **Afficher le Journal**.

Pour consulter ultérieurement un journal d'analyse ou toute infection détectée, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur l'icône en haut de la fenêtre et sélectionnez **Événements** dans le menu déroulant.
3. Dans la fenêtre **Événements**, sélectionnez **Antivirus** dans le menu déroulant correspondant.

   Cette section vous permet de trouver tous les événements d'analyse antimalware, y compris les menaces détectées par l'analyse à l'accès, les analyses lancées par un utilisateur et les modifications d'état pour les analyses automatiques.
4. Dans la liste des événements, vous pouvez consulter les analyses ayant été réalisées récemment. Cliquez sur un événement pour afficher des informations à son sujet.
5. Pour ouvrir un journal d'analyse, cliquez sur **Afficher le journal**. Le journal d'analyse s'ouvrira dans une nouvelle fenêtre.

13. CONTRÔLE PARENTAL

13.1. Comment protéger mes enfants des menaces sur Internet ?

Le Contrôle Parental de Bitdefender vous permet de limiter l'accès à Internet et à certaines applications, empêchant ainsi vos enfants de visualiser du contenu inapproprié en votre absence.

Pour configurer le contrôle parental, suivez ces étapes :

1. Créez un compte utilisateur Windows limité (standard) destiné à vos enfants. Pour plus d'informations, consultez *« Comment créer des comptes utilisateurs Windows ? »* (p. 70).
2. Assurez-vous d'être connecté à l'ordinateur en utilisant un compte administrateur. Seuls les utilisateurs ayant des droits d'administrateur sur le système peuvent avoir accès et configurer le contrôle parental.
3. Configurer le contrôle parental du compte utilisateur Windows utilisé par vos enfants.
   a. Ouvrez la fenêtre de Bitdefender.
   b. Accédez au panneau **Vie privée**.
   c. Sous le module **Contrôle Parental**, sélectionnez **Configurer**.

      Vérifiez que vous êtes connecté à votre compte MyBitdefender.
   d. Le tableau de bord du contrôle parental s'ouvrira dans une nouvelle fenêtre. Vous pouvez consulter et configurer ici les paramètres du contrôle parental.
   e. Cliquez sur **Ajouter un enfant** sur le menu de gauche.
   f. Indiquez le nom et l'âge de l'enfant dans l'onglet **Profil**. Si vous précisez l'âge de l'enfant, des paramètres considérés comme étant adaptés à cet âge seront automatiquement chargés, basés sur les normes de développement de l'enfant.

Vérifiez les activités de vos enfants et modifiez les paramètres du contrôle parental à l'aide de MyBitdefender depuis tout ordinateur ou appareil mobile connecté à Internet.

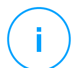
Pour des informations détaillées sur l'utilisation du contrôle parental, consultez *« Contrôle parental »* (p. 161).

13.2. Comment limiter l'accès à Internet pour mon enfant ?

Une fois le contrôle parental configuré, vous pouvez facilement bloquer l'accès à Internet à des périodes bien définies.

Le Contrôle Parental de Bitdefender vous permet de contrôler l'utilisation d'Internet de vos enfants même lorsque vous n'êtes pas chez vous.

Pour limiter l'accès à Internet à certaines heures de la journée, suivez ces étapes :

1. Sur tout périphérique avec un accès à Internet, ouvrez un navigateur Web.
2. Allez à :https://my.bitdefender.com
3. Connectez-vous à votre compte à l'aide de votre nom d'utilisateur et de votre mot de passe.
4. Cliquez sur **Contrôle Parental** pour accéder au tableau de bord.
5. Sélectionnez le profil de votre enfant dans le menu de gauche.
6. Cliquez  sur le panneau **Web** pour accéder à la fenêtre **Activité Web**.
7. Cliquez sur **Planifier**.
8. Sélectionnez dans la grille les intervalles de temps pendant lesquels l'accès à Internet est bloqué.Vous pouvez cliquer sur des cellules individuelles pour choisir des heures ou cliquer et faire glisser la souris sur plusieurs cellules pour bloquer de plus longues périodes.
9. Cliquez sur le bouton **Sauvegarder**.

Note
Bitdefender effectuera des mises à jour toutes les heures même si l'accès à Internet est bloqué.

13.3. Comment empêcher mon enfant d'accéder à un site Web ?

Le Contrôle Parental de Bitdefender vous permet de contrôler le contenu auquel accède votre enfant lorsqu'il utilise l'ordinateur et de bloquer l'accès à un site web même lorsque vous n'êtes pas chez vous.

Pour bloquer l'accès à un site Web, procédez comme suit :

1. Sur tout périphérique avec un accès à Internet, ouvrez un navigateur Web.
2. Allez à :https://my.bitdefender.com
3. Connectez-vous à votre compte à l'aide de votre nom d'utilisateur et de votre mot de passe.
4. Cliquez sur **Contrôle Parental** pour accéder au tableau de bord.
5. Sélectionnez le profil de votre enfant dans le menu de gauche.
6. Cliquez sur le panneau **Web** pour accéder à la fenêtre **Activité Web**.
7. Cliquez sur **Liste noire/Liste blanche**.
8. Indiquez le site Web dans le champ correspondant.
9. Cliquez sur **Bloquer** pour ajouter le site Web à la liste.
10. Sélectionnez dans la grille les intervalles de temps pendant lesquels l'accès est autorisé. Vous pouvez cliquer sur des cellules individuelles pour choisir des heures ou cliquer et faire glisser la souris sur plusieurs cellules pour bloquer de plus longues périodes.

    Cliquez sur le bouton **OK**.
11. Si vous changez d'avis, sélectionnez le site Web et cliquez sur le bouton **Supprimer** correspondant.

13.4. Comment empêcher mon enfant de jouer à un jeu ?

Le Contrôle Parental de Bitdefender vous permet de contrôler le contenu auquel votre enfant accède lorsqu'il utilise l'ordinateur.

Si vous avez besoin de limiter l'accès à un jeu ou à une application, vous pouvez utiliser le Contrôle Parental de Bitdefender même losque vous n'êtes pas chez vous.

Pour bloquer l'accès à un jeu, procédez comme suit :

1. Sur tout périphérique avec un accès à Internet, ouvrez un navigateur Web.
2. Allez à :https://my.bitdefender.com
3. Connectez-vous à votre compte à l'aide de votre nom d'utilisateur et de votre mot de passe.
4. Cliquez sur **Contrôle Parental** pour accéder au tableau de bord.
5. Sélectionnez le profil de votre enfant dans le menu de gauche.
6. Cliquez sur le panneau **Applications** pour accéder à la fenêtre **Activité des Applications**.
7. Cliquez sur **Liste noire**.
8. Tapez (ou copiez-collez) le chemin vers l'exécutable dans le champ correspondant.
9. Cliquez sur **Bloquer** pour ajouter l'application aux **Applications bloquées**.
10. Si vous changez d'avis, cliquez sur le bouton **Autoriser** correspondant.

13.5. Comment créer des comptes utilisateurs Windows ?

Un compte utilisateur Windows est un profil unique qui inclut tous les paramètres, privilèges et fichiers personnels de chaque utilisateur. Les comptes Windows permettent à l'administrateur des PC de contrôler l'accès de chaque utilisateur.

Il s'avère pratique de créer des comptes utilisateur lorsque le PC est utilisé à la fois par les parents et les enfants ; un parent peut créer des comptes pour chaque enfant.

Choisissez le système d'exploitation que vous avez, afin de savoir comment créer des comptes Windows.

Windows XP :

1. Connectez-vous à votre ordinateur en tant qu'administrateur.
2. Cliquez sur Démarrer, Panneau de configuration puis sur Comptes d'utilisateur.
3. Cliquez sur Créer un nouveau compte.

4. Saisissez le nom de l'utilisateur. Vous pouvez utiliser le nom complet de la personne, son prénom ou surnom. Cliquez ensuite sur Suivant.
5. Pour le type de compte, choisissez Limité puis Créer un compte. Les comptes limités sont adaptés aux enfants car ils ne peuvent pas faire de modification globale dans le système ni installer certaines applications.
6. Votre nouveau compte aura été créé et apparaîtra dans l'écran Gérer les comptes.

Windows Vista ou Windows 7 :

1. Connectez-vous à votre ordinateur en tant qu'administrateur.
2. Cliquez sur Démarrer, Panneau de configuration puis sur Comptes d'utilisateur.
3. Cliquez sur Créer un nouveau compte.
4. Saisissez le nom de l'utilisateur. Vous pouvez utiliser le nom complet de la personne, son prénom ou surnom. Cliquez ensuite sur Suivant.
5. Pour le type de compte, cliquez sur Standard puis sur Créer un compte. Les comptes limités sont adaptés aux enfants car ils ne peuvent pas faire de modification globale dans le système ni installer certaines applications.
6. Votre nouveau compte aura été créé et apparaîtra dans l'écran Gérer les comptes.

Windows 8:

1. Connectez-vous à votre ordinateur en tant qu'administrateur.
2. Placez votre souris dans l'angle supérieur droit de l'écran, cliquez sur Paramètres puis sur Modifier les paramètres du PC.
3. Cliquez sur Utilisateurs dans le menu de gauche puis cliquez sur Ajouter un utilisateur.

   Vous pouvez créer un compte Microsoft ou un compte Local. Lisez la description de chaque type de compte et suivez les instructions à l'écran pour créer un nouveau compte.



Note

Maintenant que vous avez ajouté de nouveaux comptes utilisateurs, vous pouvez créer des mots de passe pour ces comptes.

13.6. Comment supprimer un profil enfant

Si vous souhaitez supprimer un profil enfant existant, procédez comme suit :

1. Sur tout périphérique avec un accès à Internet, ouvrez un navigateur Web.
2. Allez à : https://my.bitdefender.com.
3. Connectez-vous à votre compte à l'aide de votre nom d'utilisateur et de votre mot de passe.
4. Cliquez sur **Contrôle Parental** pour accéder au tableau de bord.
5. Sélectionnez le profil enfant que vous souhaitez supprimer dans le menu de gauche.
6. Cliquez sur **Paramètres du compte**.
7. Cliquez sur **Supprimer le profil**.
8. Cliquez sur **OK**.

14. PROTECTION VIE PRIVÉE

14.1. Comment vérifier que ma transaction en ligne est sécurisée ?

Pour assurer la confidentialité de vos opérations en ligne, vous pouvez utiliser le navigateur fourni par Bitdefender pour protéger vos transations et applications bancaires.

Bitdefender Safepay™ est un navigateur sécurisé conçu pour protéger vos informations bancaires, votre numéro de compte et toutes les autres données confidentielles que vous pouvez saisir lorsque vous accédez à différents sites en ligne.

Pour assurer la sécurité et la confidentialité de vos activités en ligne, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton d'action **Safepay** à droite de la fenêtre.
3. Cliquez sur le bouton pour accéder au **Clavier virtuel**.
4. Utilisez le **Clavier virtuel** lorsque vous tapez des informations confidentielles telles que des mots de passe.

14.2. Comment protéger mon compte Facebook ?

Safego est une application Facebook développée par Bitdefender pour protéger votre compte de réseau social.

Son rôle consiste à analyser les liens que vous recevez de la part de vos amis sur Facebook et à surveiller les paramètres de confidentialité de votre compte.

Pour accéder à Safego à partir de votre produit Bitdefender, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Outils**.
3. Sous le module **Safego**, sélectionnez **Activer pour Facebook**.

   Vous serez dirigé vers votre compte.

4. Utilisez vos informations de connexion Facebook pour vous connecter à l'application Safego.
5. Autoriser Safego à accéder à votre compte Facebook.

14.3. Comment protéger mes informations personnelles ?

Pour vous assurer qu'aucune donnée à caractère personnel ne quitte votre ordinateur sans votre accord, vous devez créer des règles de protection des données. Les règles de protection des données indiquent les informations à bloquer.

Pour créer une règle de Protection des données, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Vie privée**.
3. Cliquez sur le module **Données**.
4. Si la **Protection des données** est désactivée, activez-la à l'aide du bouton correspondant.
5. Sélectionnez l'option **Ajouter une règle** pour lancer l'assistant de Protection des données.
6. Suivez les étapes de l'assistant.

14.4. Comment supprimer définitivement un fichier avec Bitdefender ?

Si vous souhaitez supprimer définitivement un fichier de votre système, vous avez besoin de supprimer physiquement les données de votre disque dur.

Le Destructeur de fichiers Bitdefender vous aidera à détruire rapidement des fichiers ou dossiers de votre ordinateur à l'aide du menu contextuel de Windows, en procédant comme suit :

1. Faites un clic droit sur le fichier ou le dossier que vous souhaitez supprimer définitivement, pointez sur Bitdefender et sélectionnez **Destructeur de fichiers**.
2. Une fenêtre de confirmation s'affichera. Cliquez sur **Oui** pour lancer l'assistant du destructeur de fichiers.

3. Patientez jusqu'à ce que Bitdefender ait terminé de détruire les fichiers.
4. Les résultats sont affichés. Cliquez sur **Fermer** pour quitter l'assistant.

15. OPTIMISATION

15.1. Comment améliorer les performances de mon système ?

Les performances système dépendent entre autres de la configuration matérielle, comme la charge du processeur, l'utilisation de la mémoire et l'espace sur le disque dur. Il est aussi lié directement à votre configuration logicielle et à la gestion de vos données.

Voici les principales actions que vous pouvez appliquer avec Bitdefender pour améliorer la vitesse et les performances de votre système :

« *Défragmentez votre disque dur* » (p. 76)

« *Optimisez les performances de votre système d'un simple clic* » (p. 76)

« *Analysez votre système régulièrement* » (p. 77)

15.1.1. Défragmentez votre disque dur

Nous vous recommandons de défragmenter le disque dur afin d'accéder aux fichiers plus rapidement et d'améliorer la performance globale du système. La défragmentation vous aide à réduire la fragmentation des fichiers et améliore les performances de votre système.

Pour lancer la défragmentation, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Outils**.
3. Sous le panneau **Optimisation**, sélectionnez **Défragmentation**.
4. Suivez les étapes de l'assistant.

Pour plus d'informations sur le module Défragmenteur de disque, reportez-vous à « *Défragmenter des volumes de disque dur* » (p. 184).

15.1.2. Optimisez les performances de votre système d'un simple clic

L'option Optimisation en 1 clic vous permet d'améliorer rapidement les performances de votre système en analysant, détectant et supprimant les fichiers inutiles.

Pour lancer le processus d'Optimisation en 1 clic, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Outils**.
3. Sous le module **Optimisation**, sélectionnez **Optimisation en 1 clic**.
4. Laissez Bitdefender rechercher les fichiers qui peuvent être supprimés puis cliquez sur le bouton **Optimiser** pour terminer le processus.

Vous pouvez également cliquer sur le bouton d'action **Optimisation** dans l'interface de Bitdefender.

Pour plus d'informations sur comment améliorer la vitesse de votre ordinateur d'un simple clic, veuillez vous reporter à *« Optimisation de la vitesse de votre système d'un simple clic »* (p. 180).

15.1.3. Analysez votre système régulièrement

La vitesse de votre système et son comportement général peuvent également être affectés par des malwares.

Veillez à analyser votre système régulièrement, au moins une fois par semaine.

Il est recommandé d'utiliser l'analyse du système car elle recherche tous les types de malwares menaçant la sécurité de votre système et analyse également l'intérieur des archives.

Pour lancer l'analyse du système, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Sous le module **Antivirus**, sélectionnez **Analyse du Système**.
4. Suivez les étapes de l'assistant.

15.2. Comment puis-je améliorer le temps de démarrage de mon système ?

Les applications inutiles qui ralentissent le démarrage du système lorsque vous allumez votre PC peuvent être désactivées ou ouvertes ultérieurement avec l'Optimisation du démarrage ce qui vous fait gagner un temps précieux.

Pour utiliser l'Optimisation du démarrage, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Outils**.
3. Sous le module **Optimisation**, sélectionnez **Optimisation du démarrage**.
4. Sélectionnez les applications dont vous souhaitez reporter le lancement au démarrage du système.

Pour plus d'informations sur la manière d'optimiser le temps de démarrage de votre PC, reportez-vous à *« Optimisation du temps de démarrage de votre PC »* (p. 181).

16. INFORMATIONS UTILES

16.1. Comment tester ma solution antivirus ?

Pour vérifier que votre produit Bitdefender fonctionne correctement, nous vous recommandons d'utiliser le test Eicar.

Le test Eicar vous permet de vérifier votre protection antivirus à l'aide d'un fichier sûr développé à cet effet.

Pour tester votre solution antivirus, procédez comme suit :

1. Téléchargez le test à partir de la page Web officielle de l'organisme EICAR http://www.eicar.org/.
2. Cliquez sur l'onglet **Anti-Malware Testfile**.
3. Cliquez sur **Download** dans le menu de gauche.
4. Dans **Download area using the standard protocol http** cliquez sur le fichier de test **eicar.com**.
5. Vous serez informé que la page à laquelle vous essayez d'accéder contient « EICAR-Test-File (not a virus) ».

   Si vous cliquez sur **Je comprends les risques, je souhaite quand même consulter cette page**, le téléchargement du test débutera et une fenêtre pop-up de Bitdefender vous indiquera qu'un virus a été détecté.

   Cliquez sur **Plus de détails** pour obtenir plus d'informations sur cette action.

Si vous ne recevez pas d'alerte Bitdefender, nous vous recommandons de contacter Bitdefender pour obtenir de l'aide comme indiqué dans la section *« Demander de l'aide »* (p. 233).

16.2. Comment désinstaller Bitdefender ?

Si vous souhaitez désinstaller Bitdefender Internet Security 2015, procédez comme suit :

Dans **Windows XP**:

1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Ajout/Suppression de programmes**.
2. Localisez **Bitdefender Internet Security 2015** et sélectionnez **Supprimer**.

3. Cliquez sur **Supprimer** pour continuer.
4. Vous disposez à cette étape des options suivantes :

   Je souhaite le réinstaller - désinstallera complètement Bitdefender. Bitdefender 60-Second Virus Scanner ne sera pas installé.

   Je souhaite le désinstaller définitivement - désinstallera complètement Bitdefender. Bitdefender 60-Second Virus Scanner sera installé sur votre système pour vous protéger contre les malwares.

   Sélectionnez l'option souhaitée et cliquez sur **Suivant**.
5. Attendez la fin du processus de désinstallation et puis redémarrez votre système.

Dans **Windows Vista** et **Windows 7**:

1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
2. Localisez **Bitdefender Internet Security 2015** et sélectionnez **Désinstaller**.
3. Cliquez sur **Supprimer** pour continuer.
4. Vous disposez à cette étape des options suivantes :

   Je souhaite le réinstaller - désinstallera complètement Bitdefender. Bitdefender 60-Second Virus Scanner ne sera pas installé.

   Je souhaite le désinstaller définitivement - désinstallera complètement Bitdefender. Bitdefender 60-Second Virus Scanner sera installé sur votre système pour vous protéger contre les malwares.

   Sélectionnez l'option souhaitée et cliquez sur **Suivant**.
5. Attendez la fin du processus de désinstallation et puis redémarrez votre système.

Dans **Windows 8** :

1. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
2. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.

3. Localisez **Bitdefender Internet Security 2015** et sélectionnez **Désinstaller**.
4. Cliquez sur **Supprimer** pour continuer.
5. Vous disposez à cette étape des options suivantes :

   Je souhaite le réinstaller - désinstallera complètement Bitdefender. Bitdefender 60-Second Virus Scanner ne sera pas installé.

   Je souhaite le désinstaller définitivement - désinstallera complètement Bitdefender. Bitdefender 60-Second Virus Scanner sera installé sur votre système pour vous protéger contre les malwares.

   Sélectionnez l'option souhaitée et cliquez sur **Suivant**.
6. Attendez la fin du processus de désinstallation et puis redémarrez votre système.



Note

Bitdefender 60-Second Virus Scanner est une application gratuite qui utilise une technologie d'analyse dans le cloud pour détecter les programmes malveillants et les menaces en moins de 60 secondes.

16.3. Comment maintenir mon système protégé après avoir désinstallé Bitdefender ?

Lors du processus de désinstallation de Bitdefender Internet Security 2015, vous disposez de l'option **Je souhaite le désinstaller définitivement** avec la possibilité d'installer Bitdefender 60-Second Virus Scanner sur votre système.

Bitdefender 60-Second Virus Scanner est une application gratuite qui utilise une technologie d'analyse dans le cloud pour détecter les programmes malveillants et les menaces en moins de 60 secondes.

Vous pouvez continuer à utiliser l'application même si vous réinstallez Bitdefender ou si vous installez un autre programme antivirus sur votre système.

Si vous souhaitez désinstaller Bitdefender 60-Second Virus Scanner, procédez comme suit :

Dans **Windows XP**:

1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Ajout/Suppression de programmes**.
2. Localisez **Bitdefender 60-Second Virus Scanner** et sélectionnez **Supprimer**.
3. Sélectionnez **Désinstaller** à l'étape suivante et patientez jusqu'à la fin du processus.

Dans **Windows Vista** et **Windows 7**:

1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
2. Localisez **Bitdefender 60-Second Virus Scanner** et sélectionnez **Désinstaller**.
3. Sélectionnez **Désinstaller** à l'étape suivante et patientez jusqu'à la fin du processus.

Dans **Windows 8** :

1. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
2. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.
3. Sélectionnez **Bitdefender 60-Second Virus Scanner** et cliquez sur **Désinstaller**.
4. Sélectionnez **Désinstaller** à l'étape suivante et patientez jusqu'à la fin du processus.

16.4. Comment éteindre automatiquement l'ordinateur une fois l'analyse terminée ?

Bitdefender propose plusieurs tâches d'analyse que vous pouvez utiliser pour vérifier que votre système n'est pas infecté par des malwares. L'analyse de l'ensemble de l'ordinateur peut prendre plus de temps en fonction de la configuration matérielle et logicielle de votre système.

C'est pourquoi Bitdefender vous permet de configurer Bitdefender pour éteindre votre système dès que l'analyse est terminée.

Prenons l'exemple suivant : vous avez terminé d'utiliser l'ordinateur et souhaitez aller dormir. Vous aimeriez que l'ensemble de votre système fasse l'objet d'une analyse antimalware par Bitdefender.

Voici comment configurer Bitdefender pour éteindre votre système à la fin de l'analyse :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Sous le module **Antivirus**, sélectionnez **Gestion des analyses**.
4. Dans la fenêtre **Gérer les tâches d'analyse**, cliquez sur **Nouvelle tâche personnalisée** pour saisir un nom pour l'analyse et sélectionnez les emplacements à analyser.
5. Si vous souhaitez configurer les options d'analyse en détail, sélectionnez l'onglet **Avancé**.
6. Choisissez d'éteindre l'ordinateur une fois l'analyse terminée si aucune menace n'est détectée.
7. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.
8. Cliquez sur **Démarrer l'analyse**.

Si aucune menace n'est détectée, l'ordinateur sera éteint.

Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer. Pour plus d'informations, consultez *« Assistant d'analyse antivirus »* (p. 103).

16.5. Comment configurer Bitdefender pour utiliser une connexion Internet par proxy ?

Si votre ordinateur se connecte à Internet via un serveur proxy, vous devez configurer Bitdefender avec les paramètres du proxy. Normalement, Bitdefender détecte et importe automatiquement les paramètres proxy de votre système.



Important

Les connexions résidentielles à Internet n'utilisent normalement pas de serveur proxy. En règle générale, vérifiez et configurez les paramètres de connexion proxy de Bitdefender lorsque aucune mise à jour n'est en cours. Si Bitdefender

peut effectuer des mises à jour, alors il est correctement configuré pour se connecter à Internet.

Pour gérer les paramètres proxy, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur l'icône en haut de la fenêtre et sélectionnez **Paramètres généraux** dans le menu déroulant.
3. Dans la fenêtre **Paramètres généraux**, sélectionnez l'onglet **Avancé**.
4. Activez l'utilisation du proxy en cliquant sur le bouton.
5. Cliquez sur le lien **Gérer proxy**.
6. Deux options permettent de définir les paramètres du proxy :

   Importer les paramètres proxy à partir du navigateur par défaut - paramètres du proxy de l'utilisateur actuel provenant du navigateur par défaut. Si le serveur proxy requiert un nom d'utilisateur et un mot de passe, vous devez les indiquer dans les champs correspondants.

   Note
   Bitdefender peut importer les paramètres proxy des principaux navigateurs, y compris des dernières versions d'Internet Explorer, de Mozilla Firefox et d'Opera.

   Paramètres proxy personnalisés - paramètres proxy que vous pouvez configurer vous-même. Voici les paramètres à spécifier:
   - **Adresse** - saisissez l'adresse IP du serveur proxy.
   - **Port** - saisissez le port utilisé par Bitdefender pour se connecter au serveur proxy.
   - **Nom d'utilisateur** - entrez le nom d'utilisateur reconnu par le serveur proxy.
   - **Mot de passe** - saisissez le mot de passe valide de l'utilisateur dont le nom vient d'être indiqué.
7. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

Bitdefender utilisera les paramètres proxy disponibles jusqu'à ce qu'il parvienne à se connecter à Internet.

16.6. Est-ce que j'utilise une version de Windows de 32 ou 64 bits ?

Pour savoir si vous disposez d'un système d'exploitation de 32 ou de 64 bits, suivez les étapes ci-dessous :

Dans **Windows XP**:

1. Cliquez sur **Démarrer**.
2. Recherchez **Poste de travail** dans le menu **Démarrer**.
3. Faites un clic droit sur **Poste de Travail**, puis sélectionnez **Propriétés**.
4. Si **Edition x64** est indiqué sous **Système**, c'est que vous exécutez la version 64 bits de Windows XP.

   Si **Edition x64** ne s'affiche pas, c'est que vous utilisez une version 32 bits de Windows XP.

Dans **Windows Vista** et **Windows 7**:

1. Cliquez sur **Démarrer**.
2. Repérez **Ordinateur** dans le menu **Démarrer**.
3. Faites un clic droit sur **Ordinateur** et sélectionnez **Propriétés**.
4. Consultez ce qui est indiqué sous **Système** afin de vérifier les informations concernant votre système.

Dans **Windows 8** :

1. Dans l'écran d'accueil Windows, localisez l'**Ordinateur** (vous pouvez, par exemple, taper « Ordinateur » directement dans l'écran d'accueil), puis faites un clic droit sur son icône.
2. Sélectionnez **Propriétés** dans le menu inférieur.
3. Regardez sous **Système** pour connaître le type de système.

16.7. Comment afficher des objets cachés dans Windows ?

Ces étapes sont utiles en cas de malwares, si vous avez besoin de détecter et de supprimer les fichiers infectés, qui peuvent être cachés.

Suivez ces étapes pour afficher les objets cachés dans Windows :

1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration.**

   Dans **Windows 8** : Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil), puis cliquez sur son icône.
2. Sélectionnez **Options des dossiers**.
3. Allez dans l'onglet **Afficher**.
4. Sélectionnez **Afficher le contenu des dossiers système** (pour Windows XP uniquement).
5. Sélectionnez **Afficher les fichiers et les dossiers cachés**.
6. Décochez **Masquer les extensions des fichiers dont le type est connu**.
7. Décochez **Masquer les fichiers protégés du système d'exploitation.**
8. Cliquez sur **Appliquer** puis sur **OK**.

16.8. Comment supprimer les autres solutions de sécurité ?

La principale raison à l'utilisation d'une solution de sécurité est d'assurer la protection et la sécurité de vos données. Mais qu'arrive-t-il quand vous avez plus d'un produit de sécurité sur le même système ?

Lorsque vous utilisez plusieurs solutions de sécurité sur le même ordinateur, le système devient instable. Le programme de désinstallation de Bitdefender Internet Security 2015 détecte d'autres programmes de sécurité et vous permet de les désinstaller.

Si vous n'avez pas supprimé les autres solutions de sécurité au cours de l'installation initiale, suivez ces étapes :

Dans **Windows XP**:

1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Ajout/Suppression de programmes**.
2. Patientez quelques instants jusqu'à ce que la liste des logiciels installés s'affiche.
3. Trouvez le nom du programme que vous souhaitez supprimer, puis sélectionnez **Supprimer**.

4. Attendez la fin du processus de désinstallation et puis redémarrez votre système.

Dans **Windows Vista** et **Windows 7**:

1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
2. Patientez quelques instants jusqu'à ce que la liste des logiciels installés s'affiche.
3. Localisez le nom du programme que vous souhaitez supprimer et sélectionnez **Désinstaller**.
4. Attendez la fin du processus de désinstallation et puis redémarrez votre système.

Dans **Windows 8** :

1. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
2. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.
3. Patientez quelques instants jusqu'à ce que la liste des logiciels installés s'affiche.
4. Localisez le nom du programme que vous souhaitez supprimer et sélectionnez **Désinstaller**.
5. Attendez la fin du processus de désinstallation et puis redémarrez votre système.

Si vous ne parvenez pas à supprimer l'autre solution de sécurité de votre système, obtenez l'outil de désinstallation sur le site web de l'éditeur ou contactez-les directement afin qu'ils vous indiquent la procédure de désinstallation.

16.9. Comment utiliser la restauration du système dans Windows ?

Si vous ne pouvez pas démarrer l'ordinateur en mode normal, lancez le mode sans échec et utilisez la Restauration du système pour restaurer un moment où vous pouviez démarrer l'ordinateur sans erreurs.

Pour effectuer la restauration du système, vous devez être connecté à Windows en tant qu'administrateur.

Pour utiliser la restauration du système, suivez ces étapes :

Dans **Windows XP**:

1. Se connecter à Windows en mode sans échec.
2. Suivez le chemin suivant à partir du menu démarrer de Windows : **Démarrer** → **Tous les programmes** → **Outils système** → **Restauration du système**.
3. Sur la page **Bienvenue dans la Restauration du système**, cliquez pour sélectionner l'option **Restaurer mon ordinateur à une date antérieure**, puis cliquez sur Suivant.
4. Suivez les étapes de l'assistant et vous devriez pouvoir démarrer le système en mode normal.

Dans **Windows Vista** et **Windows 7**:

1. Se connecter à Windows en mode sans échec.
2. Suivez le chemin suivant à partir du menu démarrer de Windows : **Tous les programmes** → **Accessoires** → **Outils système** → **Restauration du système**.
3. Suivez les étapes de l'assistant et vous devriez pouvoir démarrer le système en mode normal.

Dans **Windows 8** :

1. Se connecter à Windows en mode sans échec.
2. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
3. Sélectionnez **Récupération** puis **Ouvrir la Restauration du système**.
4. Suivez les étapes de l'assistant et vous devriez pouvoir démarrer le système en mode normal.

16.10. Comment redémarrer en mode sans échec ?

Le mode sans échec est un mode de fonctionnement de diagnostic, utilisé principalement pour résoudre des problèmes affectant le fonctionnement normal de Windows. Ce type de problèmes peut intervenir lors de conflits

de pilotes et de virus empêchant Windows de démarrer normalement. En mode sans échec, seules quelques applications fonctionnent et Windows ne charge que les pilotes de base et un minimum de composants du système d'exploitation. C'est pourquoi la plupart des virus sont inactifs lorsque Windows est en mode sans échec et qu'ils peuvent être supprimés facilement.

Pour démarrer Windows en mode sans échec :

1. Redémarrez votre système.
2. Appuyez plusieurs fois sur la touche **F8** avant que Windows ne démarre afin d'accéder au menu de démarrage.
3. Sélectionnez **Mode sans échec** dans le menu de démarrage ou **Mode sans échec avec prise en charge réseau** si vous souhaitez avoir accès à Internet.
4. Cliquez sur **Entrée** et patientez pendant que Windows se charge en mode sans échec.
5. Ce processus se termine avec un message de confirmation. Cliquez sur **OK** pour valider.
6. Pour démarrer Windows normalement, il suffit de redémarrer le système.

GÉRER VOTRE SÉCURITÉ

17. PROTECTION ANTIVIRUS

Bitdefender protège votre ordinateur contre tous les types de logiciels malveillants (virus, chevaux de Troie, spywares, rootkits, etc.).La protection offerte par Bitdefender est divisée en deux catégories:

Analyse à l'accès - empêche les nouvelles menaces d'infecter votre système.Bitdefender analysera par exemple un document Word quand vous l'ouvrez, et les e-mails lors de leur réception.

L'analyse à l'accès assure une protection en temps réel contre les malwares, et constitue un composant essentiel de tout programme de sécurité informatique.



Important

Pour empêcher l'infection de votre ordinateur par des virus, maintenez l' **analyse à l'accès** activée.

Analyse à la demande - permet de détecter et de supprimer les codes malveillants déjà présents dans le système.C'est l'analyse classique antivirus déclenchée par l'utilisateur – vous choisissez le lecteur, dossier ou fichier que Bitdefender doit analyser Bitdefender le fait – à la demande.

Bitdefender analyse automatiquement tout support amovible connecté à l'ordinateur afin de s'assurer que son accès ne pose pas de problème de sécurité. Pour plus d'informations, consultez *« Analyse automatique de supports amovibles »* (p. 107).

Les utilisateurs avancés peuvent configurer des exceptions d'analyse s'ils ne souhaitent pas que certains fichiers ou types de fichiers soient analysés. Pour plus d'informations, consultez *« Configurer des exceptions d'analyse »* (p. 109).

Lorsqu'il détecte un virus ou un autre malware, Bitdefender tente automatiquement de supprimer le code du malware du fichier infecté et de reconstruire le fichier d'origine.Cette opération est appelée désinfection.Les fichiers qui ne peuvent pas être désinfectés sont placés en quarantaine afin de contenir l'infection. Pour plus d'informations, consultez *« Gérer les fichiers en quarantaine »* (p. 112).

Si votre ordinateur a été infecté par des malwares, veuillez consulter *« Suppression des malwares de votre système »* (p. 221).Pour vous aider à supprimer les malwares qui ne peuvent pas l'être à partir du système

d'exploitation Windows, Bitdefender vous fournit le Mode de secours.Il s'agit d'un environnement de confiance, spécialement conçu pour la suppression de malwares, qui vous permet de faire redémarrer votre ordinateur indépendamment de Windows. Lorsque l'ordinateur s'exécute en Mode de Secours, les malwares Windows sont inactifs, ce qui rend leur suppression facile.

Pour vous protéger contre les applications malveillantes inconnues, Bitdefender utilise Active Virus Control, une technologie heuristique avancée, qui surveille en permanence les applications en cours d'exécution sur votre système. Le contrôle actif de virus bloque automatiquement les applications ayant un comportement similaire à celui des malwares afin de les empêcher d'endommager votre ordinateur. Des applications légitimes sont parfois bloquées. Vous pouvez dans ce cas configurer le contrôle actif de virus afin qu'il ne bloque plus ces applications en créant des règles d'exclusion. Pour en savoir plus, consultez « *Active Virus Control* » (p. 113).

17.1. Analyse à l'accès (protection en temps réel)

Bitdefender fournit une protection continue, en temps réel, contre une large gamme de malwares en analysant tous les fichiers et e-mails auxquels vous accédez.

Le réglage par défaut de la protection en temps réel assure un bon niveau de protection contre les malwares, avec un impact minimal sur les performances système.Vous pouvez facilement modifier les paramètres de la protection en temps réel selon vos besoins en choisissant un des niveaux de protection prédéfinis.Si vous êtes un utilisateur avancé, vous pouvez également configurer les paramètres d'analyse en détail en créant un niveau de protection personnalisé.

17.1.1. Activer ou désactiver la protection en temps réel

Pour activer ou désactiver la protection en temps réel contre les malwares, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Antivirus**.
4. Dans la fenêtre **Antivirus**, sélectionnez l'onglet **Résident**.

5. Cliquez sur le bouton pour activer ou désactiver l'analyse à l'accès.
6. Si vous tentez de désactiver la protection en temps réel, une fenêtre d'avertissement apparaît.Vous devez confirmer votre choix en sélectionnant dans le menu pour combien de temps vous souhaitez désactivez la protection en temps- réel. Vous pouvez désactiver la protection en temps réel pendant 5, 15 ou 30 minutes, 1 heure, en permanence ou jusqu'au redémarrage du système.La protection en temps réel sera automatiquement activée lorsque la durée sélectionnée expirera.



Avertissement

Cela peut poser un problème de sécurité important. Nous vous recommandons de désactiver la protection en temps réel pendant le moins de temps possible. Si la protection en temps réel est désactivée, vous ne serez pas protégé contre les menaces de codes malveillants.

17.1.2. Régler le niveau de protection en temps réel

Le niveau de protection en temps réel détermine les paramètres d'analyse pour la protection en temps réel.Vous pouvez facilement modifier les paramètres de la protection en temps réel selon vos besoins en choisissant un des niveaux de protection prédéfinis.

Pour régler le niveau de protection en temps réel, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Antivirus**.
4. Dans la fenêtre **Antivirus**, sélectionnez l'onglet **Résident**.
5. Déplacez le curseur sur l'échelle pour choisir le niveau de protection souhaité.Reportez-vous à la description à droite de l'échelle pour choisir le niveau de protection le plus adapté à vos besoins de sécurité.

17.1.3. Configurer les paramètres de protection en temps réel

Les utilisateurs avancés peuvent profiter des paramètres d'analyse proposés par Bitdefender.Vous pouvez configurer les paramètres de protection en temps réel en détail en créant un niveau de protection personnalisé.

Pour configurer les paramètres de la protection en temps réel, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Antivirus**.
4. Dans la fenêtre **Antivirus**, sélectionnez l'onglet **Résident**.
5. Cliquez sur **Personnaliser**.
6. Configurez les paramètres d'analyse selon vos besoins.
7. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

Informations sur les options d'analyse

Ces informations peuvent vous être utiles :

Si vous n'êtes pas familier avec certains des termes, consultez le glossaire.Vous pouvez également rechercher des informations sur Internet.

Options d'analyse à l'accès des fichiers. Vous pouvez régler Bitdefender pour analyser tous les types de fichiers auxquels vous accédez ou uniquement les applications (fichiers programmes).L'analyse de tous les fichiers accédés offre une protection maximale alors que l'analyse des applications uniquement peut être utilisée pour obtenir de meilleures performances du système.

Par défaut, les dossiers locaux et les partages réseau sont sujets à l'analyse à l'accès.Pour de meilleures performances du système, vous pouvez exclure certains emplacements du réseau de l'analyse à l'accès.

Les applications (ou les fichiers de programmes) sont bien plus vulnérables aux attaques de malwares que les autres types de fichiers.Cette catégorie comprend les extensions de fichiers suivantes :

386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam;

pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

Analyser le contenu compressé. L'analyse des fichiers compressés est un processus lent et consommant beaucoup de ressources, qui n'est donc pas recommandé pour une protection en temps réel. Les archives contenant des fichiers infectés ne constituent pas une menace immédiate pour la sécurité de votre système.Les malwares peuvent affecter votre système uniquement si le fichier infecté est extrait de l'archive et exécuté sans que la protection en temps réel ne soit activée.

Si vous décidez d'utiliser cette option, vous pouvez définir une limite de taille pour les archives à analyser à l'accès.Cochez la case correspondante et tapez la taille maximale des archives (en Mo).

Options d'analyse pour les messageries et Internet. Afin d'éviter que des malwares soient téléchargés sur votre ordinateur, Bitdefender analyse automatiquement les points d'entrée des malwares suivants :

- courriels entrants et sortants
- trafic Web

L'analyse du trafic Web peut ralentir un peu la navigation sur Internet, mais elle bloquera les malwares provenant d'Internet, y compris les téléchargements de type "drive-by".

Bien que ce ne soit pas recommandé, vous pouvez désactiver l'analyse antivirus de messagerie ou web pour améliorer les performances du système.Si vous désactivez les options d'analyse correspondantes, les courriels et les fichiers reçus ou téléchargés sur Internet ne seront pas analysés, ce qui permettra aux fichiers infectés d'être enregistrés sur votre ordinateur. Il ne s'agit pas d'une menace critique, car la protection en temps réel bloquera le malware lorsque vous tenterez d'accéder (ouvrir, déplacer, copier ou exécuter) aux fichiers infectés.

Analyser les secteurs d'amorçage. Vous pouvez paramétrer Bitdefender pour qu'il analyse les secteurs boot de votre disque dur.Ce secteur du disque dur contient le code informatique nécessaire pour faire démarrer le processus d'amorçage du système.Quand un virus infecte le secteur d'amorçage, le disque peut devenir inaccessible et il est possible que vous ne puissiez pas démarrer votre système ni accéder à vos données.

Analyser uniquement les nouveaux fichiers et ceux modifiés. En analysant uniquement les nouveaux fichiers et ceux ayant été modifiés, vous pouvez améliorer considérablement la réactivité globale du système avec un minimum de compromis en matière de sécurité.

Analyse des enregistreurs de frappe. Sélectionnez cette option pour analyser la présence d'enregistreurs de frappe sur votre système.Les enregistreurs de frappe enregistrent ce que vous tapez sur votre clavier et envoient des rapports sur Internet à une personne malveillante (un pirate informatique).Le pirate peut récupérer des informations sensibles à partir des données volées, comme vos numéros de comptes bancaires ou vos mots de passe pour les utiliser à son propre profit.

Actions appliquées à l'encontre des malwares détectés

Vous pouvez configurer les actions appliquées par la protection en temps réel.

Pour configurer les actions, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Antivirus**.
4. Dans la fenêtre **Antivirus**, sélectionnez l'onglet **Résident**.
5. Cliquez sur **Personnaliser**.
6. Configurez les paramètres d'analyse selon vos besoins.
7. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

Les actions suivantes peuvent être appliquées par la protection en temps réel dans Bitdefender :

Action automatique

Bitdefender appliquera les actions recommandées en fonction du type de fichier détecté :

Fichiers infectés . Les fichiers détectés comme étant infectés correspondent à une signature de code malveillant de la Base de Données de Signatures de Codes Malveillants Bitdefender.Bitdefender tentera de supprimer automatiquement le code malveillant du fichier infecté et de reconstituer le fichier d'origine.Cette opération est appelée désinfection.

Les fichiers qui ne peuvent pas être désinfectés sont placés en quarantaine afin de contenir l'infection. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui élimine le risque d'une infection.Pour plus d'informations, consultez *« Gérer les fichiers en quarantaine »* (p. 112).



Important

Pour certains types de malware, la désinfection n'est pas possible, car le fichier détecté est entièrement malveillant. Dans ce cas, le fichier infecté est supprimé du disque.

Fichiers suspects. Les fichiers sont détectés en tant que fichiers suspects par l'analyse heuristique.Les fichiers suspects ne peuvent pas être désinfectés, car aucune procédure de désinfection n'est disponible. Ils seront placés en quarantaine afin d'éviter une infection potentielle.

Par défaut, des fichiers de la quarantaine sont automatiquement envoyés aux laboratoires Bitdefender afin d'être analysés par les spécialistes des malwares de Bitdefender.Si la présence de malwares est confirmée, une signature est publiée afin de permettre de les supprimer.

Archives contenant des fichiers infectés.

Les archives contenant uniquement des fichiers infectés sont automatiquement supprimées.

Si une archive contient à la fois des fichiers infectés et des fichiers sains, Bitdefender tentera de supprimer les fichiers infectés s'il peut reconstituer l'archive avec les fichiers sains. Si la reconstitution de l'archive n'est pas possible, vous serez informé qu'aucune action n'a été appliquée afin d'éviter de perdre des fichiers sains.

Tout déplacer en quarantaine

Déplace les fichiers détectés dans la zone de quarantaine.Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui élimine le risque d'une infection.Pour plus d'informations, consultez *« Gérer les fichiers en quarantaine »* (p. 112).

Refuser l'accès

Dans le cas où un fichier infecté est détecté, l'accès à celui-ci est interdit.

17.1.4. Restauration des paramètres par défaut

Le réglage par défaut de la protection en temps réel assure un bon niveau de protection contre les malwares, avec un impact minimal sur les performances système.

Pour restaurer les paramètres de protection en temps réel par défaut, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Antivirus**.
4. Dans la fenêtre **Antivirus**, sélectionnez l'onglet **Résident**.
5. Cliquez sur **Par défaut**.

17.2. Analyse à la demande

L'objectif principal de Bitdefender est de conserver votre PC sans virus. Cela s'effectue en protégeant votre ordinateur des nouveaux virus par l'analyse des courriels que vous recevez et des nouveaux fichiers que vous téléchargez ou copiez sur votre système.

Il y a cependant un risque qu'un virus soit déjà logé dans votre système, avant même l'installation de Bitdefender. C'est pourquoi il est prudent d'analyser votre ordinateur après l'installation de Bitdefender. Et il encore plus prudent d'analyser régulièrement votre ordinateur contre les virus.

L'analyse à la demande est fondée sur les tâches d'analyse. Les tâches d'analyse permettent de spécifier les options d'analyse et les éléments à analyser.Vous pouvez analyser l'ordinateur quand vous le souhaitez en exécutant les tâches par défaut ou vos propres tâches d'analyse (tâches définies par l'utilisateur). Si vous souhaitez analyser certains emplacements de votre ordinateur ou configurer les options d'analyse, configurez et exécutez une analyse personnalisée.

17.2.1. Rechercher des malwares dans un fichier ou un dossier

Il est conseillé d'analyser les fichiers et les dossiers chaque fois que vous soupçonnez qu'ils peuvent être infectés.Faites un clic droit sur le fichier ou le dossier que vous souhaitez analyser, pointez sur **Bitdefender** et

sélectionnez **Analyser avec Bitdefender**.L'Assistant d'analyse antivirus s'affichera et vous guidera au cours du processus d'analyse.À la fin de l'analyse, on vous demandera de sélectionner les actions à appliquer aux fichiers détectés, le cas échéant.

17.2.2. Exécuter une analyse rapide

L'analyse rapide utilise l'analyse "sur le nuage" pour détecter les malwares présents sur votre système.La réalisation d'une analyse rapide dure généralement moins d'une minute et n'utilise qu'une petite partie des ressources du système dont a besoin une analyse antivirus classique.

Pour effectuer une analyse rapide, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Sous le module **Antivirus**, sélectionnez **Analyse Rapide**.
4. Suivez les indications de l'Assistant d'analyse antivirus pour terminer l'analyse.Bitdefender appliquera automatiquement les actions recommandées aux fichiers détectés. Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer.

17.2.3. Exécuter une analyse du système

La tâche d'analyse du système analyse l'ensemble de votre ordinateur en vue de détecter tous les types de logiciels malveillants menaçant sa sécurité : virus, logiciels-espions, publiciels, rootkits et autres.



Note

L'**analyse du système** effectue une analyse approfondie de l'ensemble du système, elle peut donc prendre un certain temps. Il est donc recommandé d'exécuter cette tâche lorsque vous n'utilisez pas votre ordinateur.

Avant d'exécuter une analyse du système, nous vous recommandons ceci :

Vérifiez que Bitdefender dispose de signatures de malwares à jour. Analyser votre ordinateur en utilisant une base de données de signatures non à jour peut empêcher Bitdefender de détecter le nouveau malware identifié depuis la mise à jour précédente.Pour plus d'informations, consultez *« Maintenir Bitdefender à jour »* (p. 44).

Fermez tous les programmes ouverts.

Si vous souhaitez analyser certains emplacements de votre ordinateur ou configurer les options d'analyse, configurez et exécutez une analyse personnalisée.Pour plus d'informations, consultez *« Configurer une analyse personnalisée »* (p. 100).

Pour exécuter une analyse du système, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Sous le module **Antivirus**, sélectionnez **Analyse du Système**.
4. Suivez les indications de l'Assistant d'analyse antivirus pour terminer l'analyse.Bitdefender appliquera automatiquement les actions recommandées aux fichiers détectés. Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer.

17.2.4. Configurer une analyse personnalisée

Pour configurer une analyse antimalware en détail et l'exécuter, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Sous le module **Antivirus**, sélectionnez **Gestion des analyses**.
4. Cliquez sur **Nouvelle tâche personnalisée** pour créer une nouvelle tâche d'analyse, et sélectionnez un emplacement à analyser.
5. Si vous souhaitez configurer les options d'analyse en détail, cliquez sur **Options d'analyse** puis sélectionnez l'onglet **Avancé.**Une nouvelle fenêtre s'affiche.Suivez ces étapes :
   a. Vous pouvez facilement configurer les options d'analyse en réglant le niveau d'analyse. Déplacez le curseur sur l'échelle pour choisir le niveau d'analyse souhaité.Reportez-vous à la description à droite de l'échelle pour identifier le niveau d'analyse le plus adapté à vos besoins.

      Les utilisateurs avancés peuvent profiter des paramètres d'analyse proposés par Bitdefender.Pour configurer les options d'analyse en détail, cliquez sur **Personnaliser**. Vous trouverez des informations à leur sujet à la fin de la section.

b. Vous pouvez aussi configurer ces options générales :

Exécuter la tâche en priorité basse . Diminue la priorité du processus d'analyse. Vous allez permettre aux autres logiciels de s'exécuter à une vitesse supérieure en augmentant le temps nécessaire pour que l'analyse soit finie.

Réduire l'assistant d'analyse dans la zone de notification . Réduit la fenêtre d'analyse dans la zone de notification. Double-cliquez sur l'icône de Bitdefender pour l'ouvrir.

Spécifiez l'action à mener si aucune menace n'a été trouvée.

c. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

6. Cliquez sur **Planifier** si vous souhaitez définir une planification pour cette tâche d'analyse.Utilisez le bouton pour activer ou désactiver la **Planification**.Sélectionnez l'une des options correspondantes pour définir une planification :

   Au démarrage du système

   Une fois

   Périodiquement

7. Sélectionnez le type d'analyse que vous souhaitez exécuter dans la fenêtre **Tâche d'analyse**.
8. Cliquez sur **Démarrer l'analyse** et suivez l'Assistant d'analyse antivirus pour terminer l'analyse. En fonction des emplacements à analyser, l'analyse peut prendre quelque temps. À la fin de l'analyse, on vous demandera de sélectionner les actions à appliquer aux fichiers détectés, le cas échéant.
9. Si vous le souhaitez, vous pouvez relancer rapidement une analyse personnalisée en cliquant sur le bouton correspondant dans la liste.

Informations sur les options d'analyse

Ces informations peuvent vous être utiles :

Si vous n'êtes pas familier avec certains des termes, consultez le glossaire.Vous pouvez également rechercher des informations sur Internet.

Analyser les fichiers. Vous pouvez régler Bitdefender pour analyser tous les types de fichiers ou uniquement les applications (fichiers programmes).L'analyse de tous les fichiers consultés offre une protection

maximale, alors que l'analyse des applications offre uniquement une analyse rapide.

Les applications (ou les fichiers de programmes) sont bien plus vulnérables aux attaques de malwares que les autres types de fichiers.Cette catégorie comprend les extensions de fichiers suivantes : 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

Options d'analyse pour les fichiers compressés. Les archives contenant des fichiers infectés ne constituent pas une menace immédiate pour la sécurité de votre système.Les malwares peuvent affecter votre système uniquement si le fichier infecté est extrait de l'archive et exécuté sans que la protection en temps réel ne soit activée. Il est toutefois recommandé d'utiliser cette option afin de détecter et de supprimer toute menace potentielle, même si celle-ci n'est pas imminente.



Note
L'analyse des fichiers compressés augmente le temps d'analyse global et demande plus de ressources système.

Analyser les secteurs d'amorçage. Vous pouvez paramétrer Bitdefender pour qu'il analyse les secteurs boot de votre disque dur.Ce secteur du disque dur contient le code informatique nécessaire pour faire démarrer le processus d'amorçage du système.Quand un virus infecte le secteur d'amorçage, le disque peut devenir inaccessible et il est possible que vous ne puissiez pas démarrer votre système ni accéder à vos données.

Analyser la mémoire. Sélectionnez cette option pour analyser les programmes s'exécutant dans la mémoire de votre système.

Analyser la base de registre. Sélectionnez cette option pour analyser les clés de registre. Le registre Windows est une base de données qui contient les paramètres et les options de configuration des composants du système d'exploitation Windows, ainsi que des applications installées.

Analyser les cookies. Sélectionnez cette option pour analyser les fichiers cookies stockés par les navigateurs sur votre ordinateur.

Analyser uniquement les nouveaux fichiers et ceux modifiés. En analysant uniquement les nouveaux fichiers et ceux ayant été modifiés, vous pouvez améliorer considérablement la réactivité globale du système avec un minimum de compromis en matière de sécurité.

Ignorer les enregistreurs de frappe commerciaux. Sélectionnez cette option si vous avez installé et utilisez un enregistreur de frappe commercial sur votre ordinateur. Les enregistreurs de frappe commerciaux sont des logiciels de surveillance légitimes dont la fonction principale consiste à enregistrer tout ce qui est tapé au clavier.

Rechercher les rootkits. Sélectionnez cette option pour rechercher des rootkits et des objets cachés à l'aide de ce logiciel.

17.2.5. Assistant d'analyse antivirus

À chaque fois que vous lancerez une analyse à la demande (par exemple en faisant un clic droit sur un dossier, en pointant sur Bitdefender et en sélectionnant **Analyser avec Bitdefender**), l'assistant de l'analyse antivirus Bitdefender s'affichera.Suivez l'assistant pour terminer le processus d'analyse.



Note

Si l'assistant d'analyse ne s'affiche pas, il est possible que l'analyse soit paramétrée pour s'exécuter en arrière-plan.Recherchez l'icône de l'avancement de l'analyse dans la zone de notification.Vous pouvez cliquer sur cette icône pour ouvrir la fenêtre d'analyse et suivre son avancement.

Étape 1 - Effectuer l'analyse

Bitdefender commence à analyser les objets sélectionnés.Vous pouvez voir des informations en temps réel sur l'état et les statistiques de l'analyse (y compris le temps écoulé, une estimation du temps restant et le nombre de menaces détectées).Pour plus d'informations, cliquez sur le lien **Plus de statistiques**.

Patientez jusqu'à ce que Bitdefender ait terminé l'analyse.L'analyse peut durer un certain temps, selon sa complexité.

Arrêt ou pause de l'analyse. Vous pouvez arrêter l'analyse à tout moment en cliquant sur **Arrêter**. Vous vous retrouverez alors à la dernière étape de l'assistant.Pour suspendre temporairement le processus d'analyse, cliquez sur **Pause**. Pour reprendre l'analyse, cliquez sur **Reprendre**.

Archives protégées par mot de passe. Lorsqu'une archive protégée par mot de passe est détectée, en fonction des paramètres de l'analyse, on peut vous demander d'indiquer son mot de passe. Les archives protégées par mot de passe ne peuvent pas être analysées si vous ne fournissez pas leur mot de passe.Voici les options proposées :

Mot de passe. Si vous souhaitez que Bitdefender analyse l'archive, sélectionnez cette option et entrez le mot de passe.Si vous ne connaissez pas le mot de passe, choisissez l'une des autres options.

Ne pas demander le mot de passe et ne pas analyser cet objet. Sélectionnez cette option pour ne pas analyser cette archive.

Ne pas analyser les éléments protégés par mot de passe. Sélectionnez cette option si vous ne voulez pas être dérangé au sujet des archives protégées par mot de passe.Bitdefender ne pourra pas les analyser, mais un rapport sera conservé dans le journal des analyses.

Sélectionnez l'option souhaitée et cliquez sur **OK** pour poursuivre l'analyse.

Étape 2 - Sélectionner des actions

À la fin de l'analyse, on vous demandera de sélectionner les actions à appliquer aux fichiers détectés, le cas échéant.



Note

Si vous lancez une analyse rapide ou une analyse complète du système, Bitdefender appliquera automatiquement les actions recommandées aux fichiers détectés pendant l'analyse. Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer.

Les objets infectés sont affichés dans des groupes, basés sur les malwares les ayant infectés.Cliquez sur le lien correspondant à une menace pour obtenir plus d'informations sur les éléments infectés.

Vous pouvez sélectionner une action globale à mener pour l'ensemble des problèmes de sécurité ou sélectionner des actions spécifiques pour chaque groupe de problèmes.Une ou plusieurs des options qui suivent peuvent apparaître dans le menu :

Action automatique

Bitdefender appliquera les actions recommandées en fonction du type de fichier détecté :

Fichiers infectés . Les fichiers détectés comme étant infectés correspondent à une signature de code malveillant de la Base de Données de Signatures de Codes Malveillants Bitdefender.Bitdefender tentera de supprimer automatiquement le code malveillant du fichier infecté et de reconstituer le fichier d'origine.Cette opération est appelée désinfection.

Les fichiers qui ne peuvent pas être désinfectés sont placés en quarantaine afin de contenir l'infection. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui élimine le risque d'une infection.Pour plus d'informations, consultez *« Gérer les fichiers en quarantaine »* (p. 112).



Important

Pour certains types de malware, la désinfection n'est pas possible, car le fichier détecté est entièrement malveillant. Dans ce cas, le fichier infecté est supprimé du disque.

Fichiers suspects. Les fichiers sont détectés en tant que fichiers suspects par l'analyse heuristique.Les fichiers suspects ne peuvent pas être désinfectés, car aucune procédure de désinfection n'est disponible. Ils seront placés en quarantaine afin d'éviter une infection potentielle.

Par défaut, des fichiers de la quarantaine sont automatiquement envoyés aux laboratoires Bitdefender afin d'être analysés par les spécialistes des malwares de Bitdefender.Si la présence de malwares est confirmée, une signature est publiée afin de permettre de les supprimer.

Archives contenant des fichiers infectés.

Les archives contenant uniquement des fichiers infectés sont automatiquement supprimées.

Si une archive contient à la fois des fichiers infectés et des fichiers sains, Bitdefender tentera de supprimer les fichiers infectés s'il peut reconstituer l'archive avec les fichiers sains. Si la reconstitution de l'archive n'est pas possible, vous serez informé qu'aucune action n'a été appliquée afin d'éviter de perdre des fichiers sains.

Supprimer

Supprime du disque les fichiers détectés.

Si des fichiers infectés sont contenus dans une archive avec des fichiers sains, Bitdefender tentera de supprimer les fichiers infectés et de reconstituer l'archive avec les fichiers sains. Si la reconstitution de l'archive n'est pas possible, vous serez informé qu'aucune action n'a été appliquée afin d'éviter de perdre des fichiers sains.

Ignorer

Aucune action ne sera menée sur les fichiers détectés.Une fois l'analyse terminée, vous pouvez ouvrir le journal d'analyse pour visualiser les informations sur ces fichiers.

Cliquez sur **Continuer** pour appliquer les actions spécifiées.

Étape 3 - Récapitulatif

Une fois que les problèmes de sécurité auront été corrigés par Bitdefender, les résultats de l'analyse apparaîtront dans une nouvelle fenêtre.Si vous souhaitez consulter des informations complètes sur le processus d'analyse, cliquez sur **Afficher journal** pour afficher le journal d'analyse.

Cliquez sur **Fermer** pour fermer la fenêtre.



Important

Dans la plupart des cas, Bitdefender désinfecte ou isole l'infection des fichiers infectés qu'il détecte.Il y a toutefois des problèmes qui ne peuvent pas être résolus automatiquement.Si cela est nécessaire, il vous sera demandé de redémarrer votre système pour terminer le processus d'installation.Pour plus d'informations et d'instructions sur la méthode permettant de supprimer des malwares manuellement, reportez-vous à *« Suppression des malwares de votre système »* (p. 221).

17.2.6. Consulter les journaux d'analyse

À chaque fois qu'une analyse est effectuée, un journal d'analyse est créé et Bitdefender enregistre les problèmes détectés dans la fenêtre Antivirus.Le

rapport d'analyse contient des informations détaillées sur le processus d'analyse, telles que les options d'analyse, la cible de l'analyse, les menaces trouvées et les actions prises à l'encontre de ces menaces.

Vous pouvez ouvrir le journal d'analyse directement à partir de l'assistant d'analyse, une fois l'analyse terminée, en cliquant sur **Afficher le Journal**.

Pour consulter ultérieurement un journal d'analyse ou toute infection détectée, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur l'icône en haut de la fenêtre et sélectionnez **Événements** dans le menu déroulant.
3. Dans la fenêtre **Événements**, sélectionnez **Antivirus** dans le menu déroulant correspondant.

   Cette section vous permet de trouver tous les événements d'analyse antimalware, y compris les menaces détectées par l'analyse à l'accès, les analyses lancées par un utilisateur et les modifications d'état pour les analyses automatiques.
4. Dans la liste des événements, vous pouvez consulter les analyses ayant été réalisées récemment.Cliquez sur un événement pour afficher des informations à son sujet.
5. Pour ouvrir le journal d'analyse, cliquez sur **Journal**.

17.3. Analyse automatique de supports amovibles

Bitdefender détecte automatiquement la connexion d'un périphérique de stockage amovible à votre ordinateur et l'analyse en tâche de fond.Ceci est recommandé afin d'empêcher que des virus ou autres malwares n'infectent votre ordinateur.

Les périphériques détectés appartiennent à l'une des catégories suivantes :

- CD ou DVD
- Des supports USB, tels que des clés flash et des disques durs externes
- disques réseau (distants) connectés

Vous pouvez configurer l'analyse automatique séparément pour chaque catégorie de périphériques de stockage. L'analyse automatique des disques réseau connectés est désactivée par défaut.

17.3.1. Comment cela fonctionne-t-il ?

Lorsqu'il détecte un périphérique de stockage amovible, Bitdefender commence à l'analyser en tâche de fond à la recherche de malwares (à condition que l'analyse automatique soit activée pour ce type de périphérique). Une icône d'analyse de Bitdefender apparaîtra dans la zone de notification.Vous pouvez cliquer sur cette icône pour ouvrir la fenêtre d'analyse et suivre son avancement.

Si la fonction Autopilote est activée, vous n'aurez pas à vous soucier de l'analyse. L'analyse sera seulement enregistrée et des informations à son sujet seront disponibles dans la fenêtre Événements.

Si Autopilote est désactivé :

1. Vous serez averti via une fenêtre contextuelle qu'un nouveau périphérique a été détecté et est en cours d'analyse.
2. Dans la plupart des cas, Bitdefender supprime automatiquement les malwares détectés ou isole les fichiers infectés en quarantaine. S'il y a des menaces non résolues après l'analyse, on vous demandera de choisir les actions à appliquer.



Note

Veuillez prendre en compte le fait qu'aucune mesure ne sera prise à l'encontre des fichiers infectés ou suspects détectés sur des CD ou DVD. De plus, aucune action ne sera appliquée à l'encontre des fichiers suspects détectés sur des lecteurs mappés du réseau si vous ne disposez pas des privilèges appropriés.

3. Lorsque l'analyse est terminée, la fenêtre des résultats de l'analyse s'affiche afin de vous informer si vous pouvez accéder aux fichiers en toute sécurité sur le support amovible.

Ces informations peuvent vous être utiles :

Soyez prudent lorsque vous utilisez un CD ou DVD infecté par des malwares, car ces malwares ne peuvent pas être supprimés du disque (le support est en lecture seule). Vérifiez que la protection en temps réel est activée pour empêcher la diffusion de malwares sur votre système. Il est recommandé de copier toutes les données essentielles du disque sur le système avant de se séparer du disque.

Bitdefender n'est parfois pas en mesure de supprimer les malwares de certains fichiers en raison de contraintes légales ou techniques. C'est le cas par exemple des fichiers archivés à l'aide d'une technologie propriétaire (car l'archive ne peut pas être recréée correctement).

Pour savoir comment traiter les malwares, reportez-vous à *« Suppression des malwares de votre système »* (p. 221).

17.3.2. Gérer l'analyse des supports amovibles

Pour gérer l'analyse automatique de supports amovibles, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Antivirus**.
4. Dans la fenêtre **Antivirus**, sélectionnez l'onglet **Exclusions**.

Pour une meilleure protection, nous vous recommandons d'activer l'analyse automatique de tous les types de périphériques de stockage amovibles.

Les options d'analyse sont déjà configurées pour que la détection soit la meilleure possible.Si des fichiers infectés sont détectés, Bitdefender essaiera de les désinfecter (supprimer le code malveillant) ou de les placer en quarantaine. Si ces actions échouent, l'assistant d'analyse antivirus vous permettra de spécifier d'autres actions à appliquer aux fichiers infectés. Les options d'analyse sont standard et vous ne pouvez pas les modifier.

17.4. Configurer des exceptions d'analyse

Bitdefender vous permet d'exclure de l'analyse certains fichiers, dossiers ou extensions de fichiers. Cette fonctionnalité est conçue pour éviter d'interférer avec votre travail et peut également contribuer à améliorer les performances du système. Les exclusions doivent être employées par des utilisateurs ayant un niveau avancé en informatique ou, sinon, selon les recommandations d'un représentant de Bitdefender.

Vous pouvez configurer des exclusions à appliquer uniquement à l'analyse à l'accès ou à la demande, ou aux deux. Les objets exclus d'une analyse à l'accès ne sont pas analysés, que ce soit vous-même ou une application qui y accédiez.



Note

Les exclusions ne sont PAS appliquées pour l’analyse contextuelle.L’analyse contextuelle est un type d’analyse à la demande : vous faites un clic droit sur le fichier ou le dossier que vous souhaitez analyser et vous sélectionnez **Analyser avec Bitdefender**.

17.4.1. Exclure de l'analyse des fichiers ou des dossiers

Pour exclure de l’analyse des fichiers ou des dossiers, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Antivirus**.
4. Dans la fenêtre **Antivirus**, sélectionnez l’onglet **Exclusions**.
5. Activez les exceptions d’analyse pour les fichiers à l’aide du bouton correspondant.
6. Cliquez sur le lien **Fichiers et dossiers exclus.**La fenêtre qui s’affiche vous permet de gérer les fichiers et dossiers exclus de l’analyse.
7. Ajoutez des exclusions en suivant ces étapes :
   a. Cliquez sur le bouton **Ajouter**, situé en haut du tableau des exclusions.
   b. Cliquez sur **Parcourir**, sélectionnez le fichier ou le dossier à exclure de l’analyse, puis cliquez sur **OK**.Vous pouvez également taper (ou copier-coller) le chemin vers le fichier ou le dossier dans le champ de saisie.
   c. Par défaut, le fichier ou dossier sélectionné est exclu à la fois de l’analyse à l’accès et à la demande. Pour modifier les conditions d’application de l’exclusion, sélectionnez l’une des autres options.
   d. Cliquez sur **Ajouter**.
8. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

17.4.2. Exclure de l'analyse des extensions de fichiers

Lorsque vous excluez de l’analyse une extension de fichier, Bitdefender n’analysera plus les fichiers avec cette extension, quel que soit leur emplacement sur votre ordinateur. L’exclusion s’applique également aux

fichiers de supports amovibles tels que les CD, les DVD, les périphériques de stockage USB ou les disques réseau.



Important
Soyez prudent lorsque vous excluez de l'analyse des extensions car celles-ci peuvent rendre votre ordinateur vulnérable aux malwares.

Pour exclure de l'analyse des extensions de fichiers, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Antivirus**.
4. Dans la fenêtre **Antivirus**, sélectionnez l'onglet **Exclusions**.
5. Activez les exceptions d'analyse pour les fichiers à l'aide du bouton correspondant.
6. Cliquez sur le lien **Extensions exclues.**La fenêtre qui s'affiche vous permet de gérer les extensions de fichiers exclues de l'analyse.
7. Ajoutez des exclusions en suivant ces étapes :
   a. Cliquez sur le bouton **Ajouter**, situé en haut du tableau des exclusions.
   b. Indiquez les extensions que vous ne souhaitez pas analyser, en les séparant par des points-virgules (;).Voici un exemple :

      txt;avi;jpg

   c. Par défaut, tous les fichiers ayant les extensions indiquées sont exclus à la fois de l'analyse à l'accès et à la demande. Pour modifier les conditions d'application de l'exclusion, sélectionnez l'une des autres options.
   d. Cliquez sur **Ajouter**.
8. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

17.4.3. Gérer les exceptions d'analyse

Si les exceptions d'analyse configurées ne sont plus nécessaires, il est recommandé de les supprimer ou de les désactiver.

Pour gérer les exceptions d'analyse, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.

2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Antivirus**.
4. Dans la fenêtre **Antivirus**, sélectionnez l'onglet **Exclusions**. Utilisez les options de la section **Fichiers et dossiers** pour gérer les exceptions d'analyse.
5. Pour supprimer ou éditer des exceptions d'analyse, cliquez sur l'un des liens. Procédez comme suit :

   Pour supprimer une entrée du tableau, sélectionnez-la et cliquez sur le bouton **Supprimer**.

   Pour modifier une entrée du tableau, double-cliquez dessus (ou sélectionnez-la et cliquez sur le bouton **Modifier**.)Une nouvelle fenêtre apparaît vous permettant de modifier l'extension ou le chemin à exclure et le type d'analyse dont vous souhaitez les exclure, le cas échéant. Effectuez les modifications nécessaires, puis cliquez sur **Modifier**.
6. Pour désactiver les exceptions d'analyse, cliquez sur le bouton correspondant.

17.5. Gérer les fichiers en quarantaine

Bitdefender isole les fichiers infectés par des malwares qu'il ne peut pas désinfecter et les fichiers suspects dans une zone sécurisée nommée quarantaine. Quand un virus est en quarantaine, il ne peut faire aucun dégât car il ne peut ni être exécuté, ni être lu.

Par défaut, des fichiers de la quarantaine sont automatiquement envoyés aux laboratoires Bitdefender afin d'être analysés par les spécialistes des malwares de Bitdefender.Si la présence de malwares est confirmée, une signature est publiée afin de permettre de les supprimer.

Bitdefender analyse également les fichiers en quarantaine après chaque mise à jour de signatures de malware.Les fichiers nettoyés sont automatiquement remis à leur emplacement d'origine.

Pour consulter et gérer les fichiers de la quarantaine, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Antivirus**.
4. Dans la fenêtre **Antivirus**, sélectionnez l'onglet **Quarantaine**.

5. Les fichiers en quarantaine sont gérés automatiquement par Bitdefender en fonction des paramètres de quarantaine par défaut. Bien que ce ne soit pas recommandé, vous pouvez régler les paramètres de quarantaine en fonction de vos préférences.

   Analyser la quarantaine après la mise à jour des définitions de virus

   Maintenez cette option activée pour analyser automatiquement les fichiers en quarantaine après chaque mise à jour des définitions de virus.Les fichiers nettoyés sont automatiquement remis à leur emplacement d'origine.

   Envoyer les fichiers suspects de la quarantaine pour analyse

   Maintenez cette option activée pour envoyer automatiquement les fichiers de la quarantaine aux laboratoires de Bitdefender.Les échantillons seront analysés par les spécialistes malwares de Bitdefender.Si la présence de malwares est confirmée, une signature est publiée afin de permettre de les supprimer.

   Supprimer le contenu datant de plus de {30} jours

   Par défaut, les fichiers placés en quarantaine depuis plus de 30 jours sont automatiquement supprimés.Si vous souhaitez modifier ce délai, entrez une nouvelle valeur dans le champ correspondant.Pour désactiver la suppression automatique des fichiers de la quarantaine selon la date, tapez 0.

6. Pour supprimer un fichier en quarantaine, sélectionnez-le, puis cliquez sur le bouton **Supprimer**.Si vous souhaitez restaurer un fichier mis en quarantaine à son emplacement d'origine, sélectionnez-le, puis cliquez sur **Restaurer**.

17.6. Active Virus Control

Bitdefender Le contrôle actif de virus est une technologie de détection proactive innovante qui utilise des méthodes heuristiques de pointe pour détecter de nouvelles menaces potentielles en temps réel.

Le contrôle actif de virus surveille en permanence les applications en cours d'exécution sur l'ordinateur, à la recherche d'actions ressemblant à celles des malwares. Chacune de ces actions est notée et un score global est calculé pour chaque processus. Lorsque la note globale d'un processus atteint un seuil donné, le processus est considéré comme malveillant et est automatiquement bloqué.

Si la fonction Autopilote est désactivée, vous serez averti via une fenêtre contextuelle sur l'application bloquée. Sinon, l'application sera bloquée sans notification. Vous pouvez vérifier les applications détectées par Le contrôle actif de virus dans la fenêtre Événements.

17.6.1. Vérifier des applications détectées

Pour contrôler les applications détectées par le contrôle actif de virus, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur l'icône en haut de la fenêtre et sélectionnez **Événements** dans le menu déroulant.
3. Dans la fenêtre **Événements**, sélectionnez **Antivirus** dans le menu déroulant correspondant.
4. Cliquez sur un événement pour afficher des informations à son sujet.
5. Si vous considérez que l'application est fiable, vous pouvez configurer le contrôle actif de virus afin qu'il ne la bloque plus en cliquant sur **Autoriser et surveiller**.Le contrôle actif de virus continuera à surveiller les applications exclues. Si les activités suspectes d'une application exclue sont détectées, l'événement sera simplement enregistré et signalé au Cloud Bitdefender comme erreur de détection.

17.6.2. Activer ou désactiver le contrôle actif de virus

Pour activer ou désactiver le contrôle actif de virus, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Antivirus**.
4. Dans la fenêtre **Antivirus**, sélectionnez l'onglet **Résident**.
5. Cliquez sur le bouton pour activer ou désactiver le contrôle actif de virus.

17.6.3. Régler la protection Contrôle actif de virus

Si vous remarquez que le contrôle actif de virus détecte souvent des applications légitimes, optez pour un niveau de protection moins strict.

Pour régler la protection Contrôle actif de virus, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Antivirus**.
4. Dans la fenêtre **Antivirus**, sélectionnez l'onglet **Résident**.
5. Vérifiez que le contrôle actif de virus est activé.
6. Déplacez le curseur sur l'échelle pour choisir le niveau de protection souhaité.Reportez-vous à la description à droite de l'échelle pour choisir le niveau de protection le plus adapté à vos besoins de sécurité.



Note

Si vous élevez le niveau de protection, le contrôle actif de virus aura besoin de moins de signes de comportements similaires à ceux des malwares pour signaler un processus. Cela conduira au signalement d'un nombre plus important d'applications et, en même temps, à un risque plus élevé de faux positifs (des applications saines détectées comme étant malveillantes).

17.6.4. Gérer les processus exclus

Vous pouvez configurer des règles d'exceptions pour les applications de confiance afin que le contrôle actif de virus ne les bloque pas si elles effectuent des actions ressemblant à celles de malwares. Le contrôle actif de virus continuera à surveiller les applications exclues. Si les activités suspectes d'une application exclue sont détectées, l'événement sera simplement enregistré et signalé au Cloud Bitdefender comme erreur de détection.

Pour gérer les exclusions de processus du contrôle actif de virus, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Antivirus**.
4. Dans la fenêtre **Antivirus**, sélectionnez l'onglet **Exclusions**.
5. Cliquez sur le lien **Processus exclus**.Dans la fenêtre qui apparaît, vous pouvez gérer les exclusions de processus du contrôle actif de virus.



Note
Lex exclusions de processus s’appliquent également à la Détection d’Intrusion.

6. Ajoutez des exclusions en suivant ces étapes :
   a. Cliquez sur le bouton **Ajouter**, situé en haut du tableau des exclusions.
   b. Cliquez sur **Parcourir**, sélectionnez l’application que vous souhaitez exclure, puis cliquez sur **OK**.
   c. Gardez l’option **Autoriser** sélectionnée pour empêcher le contrôle actif de virus de bloquer l’application.
   d. Cliquez sur **Ajouter**.
7. Pour supprimer ou éditer des exclusions, procédez comme suit :

   Pour effacer un objet de la liste, sélectionnez le et cliquez sur le bouton **Effacer**.

   Pour modifier une entrée du tableau, double-cliquez dessus (ou sélectionnez-la) et cliquez sur le bouton **Modifier**.Effectuez les modifications nécessaires, puis cliquez sur **Modifier**.
8. Enregistrer les modifications et fermer la fenêtre.

18. ANTISPAM

Le spam est un terme utilisé pour décrire les e-mails non sollicités. Le spam est un problème croissant, à la fois pour les particuliers et les entreprises. Vous ne voudriez pas que vos enfants tombent sur certains e-mails, vous pourriez perdre votre travail (pour une perte de temps trop grande ou parce que vous recevez trop de messages à caractère pornographique sur votre e-mail professionnel) et vous ne pouvez pas empêcher les gens d'en envoyer. L'idéal serait de pouvoir arrêter de les recevoir. Malheureusement, le spam revêt un large éventail de formes et de tailles, et il en existe beaucoup.

Bitdefender Antispam utilise des innovations technologiques de pointe et des filtres antispam répondant aux normes industrielles qui permettent d'éliminer les spams avant qu'ils n'atteignent la boîte aux lettres de l'utilisateur.Pour plus d'informations, consultez « *Aperçu de l'antispam* » (p. 118).

La protection Bitdefender Antispam est disponible seulement pour les clients de messagerie configurés pour recevoir des e-mails via le protocole POP3.POP3 est l'un des protocoles les plus utilisés pour télécharger des e-mails à partir d'un serveur de messagerie.



Note

Bitdefender ne fournit pas de protection antispam pour les comptes de messagerie auxquels vous accédez via un service de webmail.

Les messages de spam détectés par Bitdefender sont marqués avec le préfixe [spam] dans la ligne Objet.Bitdefender place automatiquement les messages de spam dans un dossier spécifique, comme indiqué :

Dans Microsoft Outlook, les messages de spam sont placés dans le dossier **Spam**, situé dans le dossier **Éléments supprimés**.Le dossier **Spam** est créé lors de l'installation de Bitdefender.

Dans Outlook Express et Windows Mail, les messages de spam sont placés directement dans **Éléments Supprimés**.

Dans Mozilla Thunderbird, les messages de spam sont placés dans le dossier **Spam**, situé dans le dossier **Corbeille**.Le dossier **Spam** est créé lors de l'installation de Bitdefender.

Si vous utilisez d'autres clients de messagerie, vous devez créer une règle pour déplacer les e-mails signalés comme étant du [spam] par Bitdefendervers un dossier de quarantaine personnalisé.

18.1. Aperçu de l'antispam

18.1.1. Filtres AntiSpam

Le moteur antispam de Bitdefender intègre la protection cloud et plusieurs autres filtres qui garantissent que votre boîte de réception ne contient pas de spam, tels que la Liste d'amis, la Liste des spammeurs et le Filtre jeu de caractères.

Liste d'Amis / Liste des Spammeurs

La majorité des utilisateurs communiquent régulièrement avec un groupe de personnes ou reçoivent des messages de la part d'entreprises et d'organismes d'un même domaine. En utilisant **les listes amis/spammeurs**, vous pouvez déterminer aisément de quelles personnes vous voulez recevoir des e-mails quel que soit leur contenu (amis) et de quelles personnes vous ne voulez plus en recevoir (spammeurs).



Note

Nous vous suggérons d'ajouter les noms de vos amis et leurs adresses mail à la **Liste d'Amis**. Bitdefenderne bloquera aucun de leurs messages; l'ajout des amis à la liste assure la transmission des messages légitimes.

Filtre jeu de caractères

De nombreux messages de spam sont rédigés en caractères cyrilliques et/ou asiatiques. Le filtre de caractères détecte ce type de messages et les signale comme étant du SPAM.

18.1.2. Fonctionnement de l'Antispam

Le Moteur de Bitdefender Antispam utilise tous les filtres antispam combinés pour déterminer si un e-mail doit ou non accéder à votre **Boîte de réception**.

Chaque e-mail provenant du réseau Internet est d'abord vérifié à l'aide du filtre Liste d'amis/Liste des spammeurs. Si l'adresse de l'expéditeur est identifiée dans la Liste d'amis, alors l'e-mail est directement déplacé vers votre **boîte de réception**.

Sinon, le filtre Liste des spammeurs analysera à son tour l'e-mail pour vérifier si l'adresse de l'expéditeur figure dans sa liste. En cas de correspondance, l'e-mail sera étiqueté comme étant du SPAM et déplacé dans le dossier **Spam**.

Autrement, le filtre Jeu de caractères vérifiera si l'e-mail est rédigé en caractères cyrilliques ou asiatiques. Si tel est le cas, le message sera marqué comme étant du SPAM et déplacé vers le dossier **Spam**.



Note
Si l'e-mail est marqué comme SEXUALLY EXPLICIT dans sa ligne de sujet, Bitdefender le considérera comme du SPAM.

18.1.3. Clients et protocoles de messagerie pris en charge

La protection antispam fonctionne avec tous les clients de messagerie POP3/SMTP.La barre Antispam Bitdefender ne s'affiche cependant que dans :

- Microsoft Outlook 2007 / 2010 / 2013
- Microsoft Outlook Express et Windows Mail (sur les systèmes 32 bits)
- Mozilla Thunderbird 3.0.4

18.2. Activer ou désactiver la protection antispam

La protection Antispam est activée par défaut.

Pour désactiver le module Antispam, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Antispam**.
4. Dans la fenêtre **Antispam**, cliquez sur le bouton pour activer ou désactiver l'**Antispam**.

18.3. Utilisation de la barre d'outils Antispam dans la fenêtre de votre client de messagerie

La barre d'outils Antispam se trouve dans la partie supérieure de votre client de messagerie.La barre d'outils Antispam vous aide à gérer la protection antispam directement à partir de votre client de messagerie. Vous pouvez facilement corriger Bitdefender s'il a indiqué comme SPAM un message légitime.



Important

Bitdefender s'intègre dans la plupart des clients de messagerie via une barre d'outils antispam facile à utiliser.Pour une liste complète des clients de messagerie pris en charge, veuillez vous référer à *« Clients et protocoles de messagerie pris en charge »* (p. 119).

Chaque bouton de la barre d'outils de Bitdefender sera expliqué ci-dessous:

Spam - indique que le message sélectionné est un spam. L'e-mail sera immédiatement placé dans le dossier **Spam**.Si les services cloud antispam sont activés, le message est envoyé au Cloud Bitdefender pour une analyse plus approfondie.

Pas Spam - indique que l'e-mail sélectionné n'est pas du spam et que Bitdefender ne devrait pas l'avoir signalé comme tel.Cet email sera retiré du dossier **Spam** et placé dans la **Boîte de réception**.Si les services cloud antispam sont activés, le message est envoyé au Cloud Bitdefender pour une analyse plus approfondie.



Important

Le bouton **Pas Spam** devient actif quand vous choisissez un message marqué spam par Bitdefender (ces messages se trouvent d'habitude dans le répertoire **Spam**).

Ajouter Spammeur - ajoute l'expéditeur de l'e-mail sélectionné à la liste des Spammeurs.Il se peut que vous ayez besoin de cliquer sur **OK** pour valider.Les messages provenant d'adresses qui figurent dans la liste de Spammeurs seront automatiquement considérés comme étant du [spam].

Ajouter Ami - ajoute l'expéditeur de l'e-mail sélectionné à la liste d'Amis.Il se peut que vous ayez besoin de cliquer sur **OK** pour valider.Les futurs messages provenant de cette adresse seront toujours dirigés vers votre boîte de réception quel que soit leur contenu.

Spammeurs - ouvre la liste des **Spammeurs**qui contient toutes les adresses e-mail dont vous ne voulez recevoir aucun message, quel que soit son contenu.Pour plus d'informations, consultez *« Configurer la liste des spammeurs »* (p. 123).

Amis - ouvre la **Liste d'amis** qui contient tous les emails que vous souhaitez recevoir quel qu'en soit le contenu.Pour plus d'informations, consultez *« Configurer la liste d'amis »* (p. 122).

Configuration - ouvre une fenêtre qui vous permet de configurer les filtres antispam et les paramètres de la barre d'outils.

18.3.1. Indiquer des erreurs de détection

Si vous utilisez un client de messagerie pris en charge, vous pouvez facilement corriger le filtre antispam (en indiquant quels e-mails n'auraient pas dû être signalés comme étant du [spam]). Cela contribue à améliorer considérablement l'efficacité du filtrage antispam.Suivez ces étapes :

1. Ouvrez votre client de messagerie.
2. Allez dans le dossier de courrier indésirable dans lequel les messages de spam sont placés.
3. Sélectionnez le message légitime considéré à tort comme étant du [spam] par Bitdefender.
4. Cliquez sur le bouton **Ajouter un ami** de la barre d'outils antispam Bitdefender pour ajouter l'expéditeur à la liste d'Amis.Il se peut que vous ayez besoin de cliquer sur **OK** pour valider.Les futurs messages provenant de cette adresse seront toujours dirigés vers votre boîte de réception quel que soit leur contenu.
5. Cliquez sur le bouton **Pas Spam** de la barre d'outils antispam de Bitdefender (généralement située dans la partie supérieure de la fenêtre du client de messagerie). Le message d'e-mail sera placé dans la boîte de réception.

18.3.2. Indiquer les messages de spam non détectés

Si vous utilisez un client de messagerie pris en charge, vous pouvez facilement indiquer quels e-mails auraient dû être détectés comme étant du spam. Cela contribue à améliorer considérablement l'efficacité du filtrage antispam.Suivez ces étapes :

1. Ouvrez votre client de messagerie.
2. Allez dans la boîte de Réception.
3. Sélectionnez les messages de spam non détectés.
4. Cliquez sur le bouton **Spam** de la barre d'outils antispam de Bitdefender (généralement située dans la partie supérieure de la fenêtre du client de messagerie). Ils sont immédiatement signalés comme étant du [spam] et déplacés vers le dossier du courrier indésirable.

18.3.3. Configurer les paramètres de la barre d'outils

Pour configurer les paramètres de la barre d'outils antispam de votre client de messagerie, cliquez sur le bouton **Configuration** de la barre d'outils puis sur l'onglet **Paramètres de la barre d'outils**.

Vous disposez des options suivantes :

Placer le message dans les éléments supprimés (uniquement pour Microsoft Outlook Express / Windows Mail)



Note
Dans Microsoft Outlook / Mozilla Thunderbird, les messages de spam détectés sont automatiquement placés dans un dossier Spam, situé dans le dossier Éléments supprimés / Corbeille.

Signaler les messages spam comme 'lus' - signale automatiquement les messages spam comme lus, de manière à éviter le dérangement que provoque leur arrivée.
Vous pouvez choisir d'afficher ou non des fenêtres de confirmation lorsque vous cliquez sur les boutons **Ajouter spammeur** et **Ajouter ami** de la barre d'outils antispam.

Les fenêtres de confirmation peuvent empêcher d'ajouter accidentellement des expéditeurs d'e-mails à la liste d'Amis / de Spammeurs.

18.4. Configurer la liste d'amis

La **liste d'amis** est une liste de toutes les adresses e-mail de la part desquelles vous voulez toujours recevoir les messages, quel que soit leur contenu. Les messages de vos amis ne seront jamais considérés comme étant du spam, même si leur contenu ressemble à du spam.



Note
Tout message provenant d'une adresse contenue dans la **liste d'amis** sera automatiquement déposé dans votre boîte de réception sans autre traitement.

Pour configurer et gérer la liste d'Amis :

Si vous utilisez Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, cliquez sur le bouton **Amis** de la barre d'outils antispam Bitdefender.

Vous pouvez également procéder comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Sous le module **Antispam**, sélectionnez **Gérer les amis**.

Pour ajouter une adresse e-mail, sélectionnez l'option **Adresse e-mail**, indiquez l'adresse puis cliquez sur **Ajouter**.Syntaxe: name@domain.com.

Pour ajouter toutes les adresses e-mail d'un domaine particulier, sélectionnez l'option **Nom de domaine**, indiquez le nom de domaine puis cliquez sur **Ajouter**.Syntaxe:

@domain.com, *domain.com et domain.com - tous les messages en provenance de domain.com seront dirigés vers votre **Boîte de réception** quel que soit leur contenu;
domain - tous les messages provenant de domain (quel que soit le suffixe) seront dirigés vers votre **Boîte de réception** quel que soit leur contenu;
*com - tous les messages ayant comme suffixe du domaine com seront dirigés vers votre **Boîte de réception** quel que soit leur contenu;

Il est recommandé d'éviter d'ajouter des noms de domaines entiers, mais cela peut être utile dans certaines situations.Vous pouvez, par exemple, ajouter le domaine de messagerie électronique de la société pour laquelle vous travaillez ou les domaines de partenaires en qui vous avez confiance.

Pour retirer un élément de la liste, cliquez sur le lien correspondant **Supprimer**.Pour supprimer toutes les entrées de la liste, cliquez sur le bouton **Nettoyer**.

Vous pouvez enregistrer la liste d'amis dans un fichier afin de pouvoir l'utilisersur un autre ordinateur ou si vous réinstallez le produit.Pour enregistrer la liste d'Amis, cliquez sur le bouton **Enregistrer** et enregistrez-la à l'emplacement désiré.Le fichier aura l'extension .bwl.

Pour charger une liste d'Amis enregistrée préalablement, cliquez sur le bouton **Charger** et ouvrez le fichier .bwl correspondant.Pour supprimer le contenu de la liste en cours d'utilisation lorsque vous chargez une liste enregistrée auparavant, sélectionnez **Écraser la liste en cours**.

Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

18.5. Configurer la liste des spammeurs

La **liste des spammeurs** est une liste de toutes les adresses e-mail de la part desquelles vous ne voulez recevoir aucun message, quel que soit leur

contenu.Tout message en provenance d'une adresse de la **liste des spammeurs** sera automatiquement marqué SPAM sans autre traitement.

Pour configurer et gérer la liste des Spammeurs :

Si vous utilisez Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, cliquez sur le bouton **Spammeurs** de la barre d'outils antispam Bitdefender intégrée à votre client de messagerie.

Vous pouvez également procéder comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Sous le module **Antispam**, sélectionnez **Gérer spammeurs**.

Pour ajouter une adresse e-mail, sélectionnez l'option **Adresse e-mail**, indiquez l'adresse puis cliquez sur **Ajouter**.Syntaxe: name@domain.com.

Pour ajouter toutes les adresses e-mail d'un domaine particulier, sélectionnez l'option **Nom de domaine**, indiquez le nom de domaine puis cliquez sur **Ajouter**.Syntaxe:

@domain.com, *domain.com et domain.com - tous les messages provenant de domain.com seront étiquetés comme SPAM;
domain - tous les messages de domain (quel que soit le suffixe) seront étiquetés comme SPAM;
*com - tous les messages provenant d'un domaine avec un suffixe com seront étiquetés comme SPAM.

Il est recommandé d'éviter d'ajouter des noms de domaines entiers, mais cela peut être utile dans certaines situations.



Avertissement

N'ajoutez pas de domaines de services webmail légitimes (tels que Yahoo, Gmail, Hotmail ou d'autres) à la liste des Spammeurs. Sinon, les e-mails envoyés par les utilisateurs de ces services seront identifiés comme étant du spam. Si par exemple, vous ajoutez yahoo.com à la liste des Spammeurs, tous les e-mails provenant d'adresses yahoo.com seront identifiés comme étant du [spam].

Pour retirer un élément de la liste, cliquez sur le lien correspondant **Supprimer**.Pour supprimer toutes les entrées de la liste, cliquez sur le bouton **Nettoyer**.

Vous pouvez enregistrer la liste des spammeurs dans un fichier afin de pouvoirl'utiliser sur un autre ordinateur ou si vous réinstallez le produit.Pour enregistrer la liste des Spammeurs, cliquez sur le bouton **Enregistrer** et enregistrez-la à l'emplacement désiré.Le fichier aura l'extension .bwl.

Pour charger une liste de Spammeurs enregistrée préalablement, cliquez sur le bouton **Charger** et ouvrez le fichier .bwl correspondant.Pour supprimer le contenu de la liste en cours d'utilisation lorsque vous chargez une liste enregistrée auparavant, sélectionnez **Écraser la liste en cours**.

Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

18.6. Configurer les filtres antispam locaux

Comme cela est décrit dans « *Aperçu de l'antispam* » (p. 118), Bitdefender utilise une combinaison de divers filtres antispam pour identifier le spam.Les filtres antispam sont préconfigurés pour une protection efficace.



Important

Selon que vous recevez ou non des e-mails légitimes rédigés avec des caractères asiatiques ou cyrilliques, désactivez ou activez le paramètre bloquant automatiquement ces e-mails. Le paramètre correspondant est désactivé dans les versions localisées du programme utilisant ces jeux de caractères (par exemple, dans la version russe ou chinoise).

Pour configurer les filtres antispam locaux, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Antispam**.
4. Dans la fenêtre **Antispam**, sélectionnez l'onglet **Paramètres**.
5. Cliquez sur les boutons pour activer ou désactiver les filtres antispam locaux.

Si vous utilisez Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, vous pouvez configurer les filtres antispam locaux directement à partir de votre client de messagerie. Cliquez sur le bouton **Configuration** de la barre d'outils antispam de Bitdefender (généralement situé dans la partie supérieure de la fenêtre du client de messagerie) puis sur l'onglet **Filtres Antispam**.

18.7. Configurer les paramètres cloud

La détection « in the cloud » utilise les services Cloud de Bitdefender pour vous fournir une protection antispam efficace et toujours à jour.

La protection cloud fonctionne tant que vous maintenez Bitdefender Antispam activé.

Des échantillons d'e-mails de spam ou légitimes peuvent être envoyés au Cloud Bitdefender lorsque vous signalez des erreurs de détection ou des e-mails de spam non détectés. Cela contribue à améliorer la détection antispam de Bitdefender.

Pour configurer l'envoi d'échantillons d'e-mails au Cloud Bitdefender sélectionnez les options souhaitées en procédant comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Antispam**.
4. Dans la fenêtre **Antispam**, sélectionnez les options souhaitées dans l'onglet **Configuration**.

Si vous utilisez Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, vous pouvez configurer la détection cloud directement à partir de votre client de messagerie. Cliquez sur le bouton **Configuration** de la barre d'outils antispam de Bitdefender (généralement situé dans la partie supérieure de la fenêtre du client de messagerie) puis sur l'onglet **Configuration du Cloud**.

19. PROTECTION WEB

La protection Web de Bitdefender vous garantit une navigation sur Internet en toute sécurité en vous signalant les pages web présentant un risque de phishing.

Bitdefender fournit une protection web en temps réel pour :

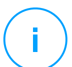
Internet Explorer
Mozilla Firefox
Google Chrome
Safari

Pour configurer les paramètres de la protection Web, les étapes sont les suivantes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Protection Web**.

Cliquez sur les boutons pour activer ou désactiver :

Affichage de la barre d'outils Bitdefender dans le navigateur web.



Note
La barre d'outils du navigateur Bitdefender n'est pas activée par défaut.

Conseiller de recherche, un composant qui évalue les résultats de vos requêtes sur les moteurs de recherche et les liens postés sur les sites Web de réseaux sociaux en plaçant une icône à côté de chaque résultat :

Nous vous déconseillons de consulter cette page Web.

Cette page Web peut contenir du contenu dangereux. Soyez prudent si vous décidez de le consulter.

Cette page peut être consultée en toute sécurité.

Conseiller de recherche évalue les résultats de recherche des moteurs de recherche Web suivants :

Google
Yahoo!
Bing
Baidu

Conseiller de recherche évalue les liens postés sur les sites de réseaux sociaux suivants :

- Facebook
- Twitter

Analyse du trafic web SSL.

Des attaques plus sophistiquées peuvent utiliser le trafic Web sécurisé pour induire en erreur leurs victimes.Nous vous recommandons donc d'activer l'analyse SSL.

Protection contre les escroqueries.

Protection contre l'hameçonnage.

Vous pouvez créer une liste de sites Web qui ne seront pas analysés par les moteurs antimalware, antiphishing et antifraude de Bitdefender.La liste ne doit contenir que des sites Web de confiance.Par exemple, ajoutez les sites Web sur lesquels vous avez l'habitude de faire vos achats en ligne.

Pour configurer et administrer les sites web à l'aide de la protection web fournie par Bitdefender, cliquez sur le lien **Liste blanche**.Une nouvelle fenêtre s'affiche.

Pour ajouter un site à la liste blanche, entrez son adresse dans le champ correspond et cliquez sur **Ajouter**.

Pour supprimer un site Web de la liste, sélectionnez-le dans la liste et cliquez sur le lien **Supprimer**.

Cliquez sur **Enregistrer** pour sauvegarder les modifications et fermer la fenêtre.

19.1. Protection Bitdefender dans le navigateur web

Bitdefender s'intègre directement et au moyen d'une barre d'outils intuitive et conviviale aux navigateurs Internet suivants :

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari

La barre d'outils de Bitdefender n'est pas votre barre d'outils de navigateur typique. La seule chose qu'il ajoute à votre navigateur est un petit bouton en haut de chaque page Web.Cliquez dessus pour voir la barre d'outils.

La barre d'outils Bitdefender contient les éléments suivants :

Résultat de la page

En fonction de la façon dont Bitdefender classifie la page web que vous affichez, l'un des résultats suivants s'affiche dans la partie gauche de la barre d'outils :

Le message "Page non sûre" apparaît sur un fond rouge - nous vous recommandons de quitter immédiatement la page Web. Pour plus d'informations sur cette menace, cliquez sur le symbole **+** sur le résultat de la page.

Le message "Nous vous recommandons d'être vigilant" apparaît sur un fond orange - le contenu de cette page Web peut être dangereux.Soyez prudent si vous décidez de le consulter.

Le message "Cette page est sûre" apparaît sur un fond vert - il s'agit d'une page sûre que vous pouvez consulter.

Bac à sable

Cliquez sur pour lancer le navigateur dans un environnement fourni par Bitdefender, l'isolant du système d'exploitation. Cela empêche les menaces de navigateur d'exploiter les vulnérabilités des navigateurs pour prendre le contrôle de votre système. Utilisez la fonction Bac à sable lorsque vous consultez des pages Web que vous suspectez de contenir des malwares.

Les fenêtres du navigateur ouvertes dans le bac à sable seront facilement identifiables grâce à leur contour modifié et à l'icône Bac à sable ajoutée au centre de la barre de titre.



Note

Le bac à sable n'est pas disponible sur les ordinateurs fonctionnant sous Windows XP.

Configuration

Cliquez sur pour sélectionner les fonctionnalités individuelles à activer ou désactiver :

Filtre anti-hameçonnage
Filtre Web antimalware
Search Advisor

Bouton marche/arrêt

Pour activer / désactiver complètement les fonctionnalités de la barre d'outils, cliquez sur sur le côté droit de la barre d'outils.

19.2. Alertes Bitdefender dans le navigateur

Lorsque vous essayez de consulter un site Web considéré comme non sûr, ce site web est bloqué et une page d'avertissement s'affiche dans votre navigateur.

La page contient des informations telles que l'URL du site web et la menace détectée.

Vous devez décider quoi faire ensuite. Voici les options proposées :

Quittez la page Web en cliquant sur **Retour en toute sécurité**.

Désactivez le blocage des pages d'hameçonnage en cliquant sur **Désactiver le filtre anti-hameçonnage**.

Désactivez le blocage des pages contenant des malwares en cliquant sur **Désactiver le filtre antimalware**.

Ajoutez la page à la liste blanche anti-hameçonnage en cliquant sur **Ajouter à la liste blanche**.Cette page ne sera plus analysée par les moteurs Antiphishing de Bitdefender.

Pour vous rendre sur le site Web, malgré l'avertissement, cliquez sur **Je comprends les risques, je souhaite quand même consulter cette page**.

20. PROTECTION DES DONNÉES

La protection des données empêche les fuites de données sensibles lorsque vous êtes en ligne.

Prenons un exemple simple : vous avez créé une règle de protection des données qui protège votre numéro de carte bancaire.Si un logiciel espion parvient à s'installer sur votre ordinateur, il ne peut pas transmettre votre numéro de carte bancaire par courriel, messages instantanés ou pages Web. De plus, vos enfants ne peuvent pas l'utiliser pour faire des achats en ligne ou le révéler à des personnes rencontrées sur Internet.

20.1. À propos de la protection des données

Qu'il s'agisse de votre adresse courriel ou de votre numéro de carte bancaire, si ces informations tombent dans de mauvaises mains vous pouvez en subir les conséquences: crouler sous les pourriels ou retrouver votre compte bancaire vide.

En se basant sur les règles que vous avez créées, la protection des données analyse le trafic Internet, de messagerie et de messagerie instantanée partant de votre ordinateur, pour y rechercher des chaînes de texte spécifiques que vous avez définies (par exemple, votre numéro de carte bancaire). En cas de correspondance, la page Web, le courriel ou le message instantané concerné est bloqué.

Vous pouvez créer des règles pour protéger toutes les informations que vous considérez comme personnelles ou confidentielle, votre numéro de téléphone, votre adresse courriel ou votre numéro de compte bancaire.Le support multi-utilisateur est fourni pour que les utilisateurs connectés sur des comptes Windows différents puissent configurer et utiliser leurs propres règles.Si votre compte Windows est un compte administrateur, les règles que vous créez peuvent être configurées pour s'appliquer également lorsque d'autres utilisateurs de l'ordinateur sont connectés à leurs comptes utilisateurs Windows.

20.2. Configurer la protection des données

Si vous souhaitez utiliser la protection des données, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Vie privée**.

3. Cliquez sur le module **Données**.
4. Vérifiez que la protection des données est activée.
5. Définissez les règles nécessaires à la protection de vos données sensibles.Pour plus d'informations, consultez *« Créer des règles de protection des données »* (p. 132).

20.2.1. Créer des règles de protection des données

Pour créer un règle, cliquez sur le bouton **Ajouter une règle** et suivez les indications de l'assistant de configuration. Vous pouvez naviguer dans l'assistant à l'aide des boutons **Suivant** et **Retour**. Pour quitter l'assistant, cliquez sur **Annuler**.

1. **Décrire la règle**

   Vous devez définir les paramètres suivants :

   Nom de la règle - saisissez le nom de la règle dans ce champ de saisie.

   Type de règle - détermine le type de règle (adresse, nom, carte bancaire, code PIN, etc.)

   Données de la règle - saisissez les données que vous voulez protéger dans ce champ de saisie. Si par exemple vous voulez protéger votre numéro de carte de crédit, saisissez ici l'intégralité ou une partie de celui-ci.

   Important
   Nous vous recommandons d'entrer au moins trois caractères de manière à éviter de bloquer par erreur des messages et des pages Web. Cependant, pour plus de sécurité, indiquez uniquement une partie des données (par exemple, seulement une partie de votre numéro de carte bancaire).

   Description de la règle - indiquez une brève description de la règle dans le champ correspondant. Puisque les données bloquées (chaines de caractères) ne sont pas affichées sous forme de texte clair quand vous accédez à la règle, la description devrait vous aider à l'identifier rapidement.

2. **Configurer les paramètres de la règle**

   a. Sélectionnez le type de trafic que laBitdefender doit analyser.

Analyse Web (trafic HTTP) - analyse le trafic Web (HTTP) et bloque les données sortantes correspondant aux données de la règle.

Analyse courriel (trafic SMTP) - analyse le trafic courriel (SMTP) et bloque les courriel sortants qui contiennent les éléments déterminés dans la règle de gestion des données.

Vous pouvez choisir d'appliquer la règle uniquement si les données de la règle correspondent à tous les mots ou à la chaîne de caractères détectée.

b. Spécifiez les utilisateurs pour lesquels la règle s'applique.

Seulement pour moi (utilisateur actuel) - la règle s'appliquera seulement à votre compte utilisateur.

Tous les utilisateurs - la règle s'appliquera à tous les comptes Windows.

Comptes utilisateurs limités - la règle s'appliquera à vous et aux comptes Windows limités.

Cliquez sur **Terminer**. La règle apparaîtra dans le tableau.

Désormais, toute tentative d'envoi de données visées par la règle via les protocoles sélectionnés échouera. Une entrée apparaîtra dans le fenêtre Événements indiquant que Bitdefender a bloqué l'envoi de contenu lié à l'identité.

20.3. Gestion des règles

Pour gérer les règles de protection des données :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Vie privée**.
3. Cliquez sur le module **Données**.

Vous pouvez voir les règles existantes dans le tableau.

Pour supprimer une règle, sélectionnez-la, puis cliquez sur le bouton **Supprimer**.

Pour modifier une règle, sélectionnez-la et cliquez sur le bouton **Modifier la règle**. Une nouvelle fenêtre s'affiche.Vous pouvez modifier ici le nom, la description et les paramètres de la règle (type, données et trafic). Cliquez **OK** pour sauvegarder les changements.

20.4. Supprimer définitivement des fichiers

Lorsque vous supprimez un fichier, vous ne pouvez plus y accéder par le chemin habituel. Toutefois, ce fichier continue d'être stocké sur le disque dur jusqu'à ce qu'il soit remplacé lors de la copie de nouveaux fichiers.

Le Destructeur de Fichiers Bitdefender vous aidera à supprimer définitivement des données en les supprimant physiquement de votre disque dur.

Vous pouvez détruire rapidement des fichiers ou dossiers de votre ordinateur à l'aide du menu contextuel de Windows, en procédant comme suit :

1. Faites un clic droit sur le fichier ou le dossier que vous souhaitez supprimer définitivement.
2. Sélectionnez **Bitdefender** > **Destructeur de fichiers** dans le menu contextuel qui apparaît.
3. Une fenêtre de confirmation s'affichera. Cliquez sur **Oui** pour lancer l'assistant du destructeur de fichiers.
4. Patientez jusqu'à ce que Bitdefender ait terminé de détruire les fichiers.
5. Les résultats sont affichés.Cliquez sur **Fermer** pour quitter l'assistant.

Vous pouvez également détruire des fichiers à partir de l'interface de Bitdefender.

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Vie privée**.
3. Sous le module **Données**, sélectionnez **Destructeur de fichiers**.
4. Suivez l'assistant du destructeur de fichiers :
   a. **Sélectionnez un élément**

      Ajoutez les fichiers ou les dossiers que vous souhaitez supprimer définitivement.

   b. **Destruction des fichiers**

      Patientez jusqu'à ce que Bitdefender ait terminé de détruire les fichiers.

   c. **Résultats**

      Les résultats sont affichés.Cliquez sur **Fermer** pour quitter l'assistant.

21. VULNÉRABILITÉ

Une étape importante permettant de préserver votre ordinateur contre les personnes malveillantes et les menaces est de maintenir à jour votre système d'exploitation et vos principales applications.Vous devriez également envisager de désactiver les paramètres Windows qui rendent le système plus vulnérable aux malwares. De plus, afin de prévenir tout accès physique non autorisé à votre ordinateur, il est recommandé d'utiliser des mots de passe complexes (qui ne peuvent pas être devinés trop facilement) pour chaque compte utilisateur Windows.

Bitdefender recherche automatiquement les vulnérabilités de votre système et vous les signale.Les vulnérabilités du Système peuvent être :

- la présence sur votre ordinateur d'applications non à jour
- des mises à jour Windows manquantes
- des mots de passe non sécurisés de comptes utilisateurs Windows

Bitdefender fournit deux manières simples de corriger les vulnérabilités de votre système :

- Vous pouvez rechercher des vulnérabilités sur votre système et les corriger pas à pas à l'aide de l'option **Analyse de Vulnérabilité**.
- La surveillance des vulnérabilités automatique vous permet de vérifier et de corriger les vulnérabilités détectées dans la fenêtre Événements.

Nous vous recommandons de vérifier et de corriger les vulnérabilités du système toutes les semaines, ou une fois toutes les deux semaines.

21.1. Analyser votre système à la recherche de vulnérabilités

Pour corriger les vulnérabilités du système à l'aide de l'option Analyse de Vulnérabilité, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Sous le module **Vulnérabilité**, sélectionnez **Analyse de Vulnérabilité**.

4. Patientez jusqu'à ce que Bitdefender ait analysé votre système à la recherche de vulnérabilités. Pour arrêter le processus d'analyse, cliquez sur le bouton **Ignorer** en haut de la fenêtre.

   a. **Mises à jour d'applications**

      Si une application n'est pas à jour, cliquez sur le lien indiqué pour télécharger la dernière version.

      Cliquez sur **Afficher les détails** pour voir des informations sur l'application ayant besoin d'être mise à jour.

   b. **Mises à jour Windows**

      Cliquez sur **Afficher les détails** pour voir la liste des mises à jour Windows critiques qui ne sont pas installées sur votre ordinateur.

      Pour lancer l'installation des mises à jour sélectionnées, cliquez sur **Installer les mises à jour**.Veuillez noter que l'installation des mises à jour peut durer un certain temps et que certaines peuvent nécessiter un redémarrage du système. Si nécessaire, redémarrez le système dès que possible.

   c. **Mots de passe vulnérables**

      Vous pouvez voir une liste des comptes utilisateur Windows configurés sur votre ordinateur ainsi que le niveau de protection que leur mot de passe respectif apportent.

      Cliquez sur **Afficher les détails** pour modifier les mots de passe vulnérables.Vous pouvez choisir entre demander à l'utilisateur de modifier le mot de passe lors de sa prochaine connexion ou modifier le mot de passe par vous-même immédiatement. Pour avoir un mot de passe sécurisé, utilisez un mélange de lettres majuscules, minuscules, de nombres et de caractères spéciaux (comme par exemple #, $ ou @).

L'angle supérieur droit de la fenêtre vous permet de filtrer les résultats en fonction de vos préférences.

21.2. Utiliser la surveillance des vulnérabilités automatique

Bitdefender analyse régulièrement votre système à la recherche de vulnérabilités, en tâche de fond, et enregistre les problèmes détectés dans la fenêtre Événements.

Pour vérifier et corriger les problèmes détectés, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur l'icône en haut de la fenêtre et sélectionnez **Événements** dans le menu déroulant.
3. Dans la fenêtre **Événements**, sélectionnez **Vulnérabilité**.
4. Vous pouvez consulter des informations détaillées au sujet des vulnérabilités du système détectées. En fonction du problème, procédez comme suit pour corriger une vulnérabilité spécifique :

   Si des mises à jour Windows sont disponibles, cliquez sur **Mettre à jour**.

   Si une application n'est pas à jour, cliquez sur **Mettre à jour maintenant** pour trouver un lien vers la page Web du fournisseur d'où vous pourrez installer la dernière version de l'application.

   Si un compte utilisateur Windows a un mot de passe vulnérable, cliquez sur **Changer de mot de passe** pour obliger l'utilisateur à modifier son mot de passe lors de la prochaine connexion ou pour changer le mot de passe par vous-même.Pour avoir un mot de passe sécurisé, utilisez un mélange de lettres majuscules, minuscules, de nombres et de caractères spéciaux (comme par exemple #, $ ou @).

   Si la fonctionnalité AutoRun de Windows est activée, cliquez sur **Désactiver** pour la désactiver.

Pour configurer les paramètres de surveillance des vulnérabilités, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Vulnérabilité**.
4. Cliquez sur le bouton pour activer ou désactiver l'analyse de vulnérabilité.



Important

Pour être automatiquement averti(e) en cas de vulnérabilités du système ou des applications, veuillez garder l'option **Analyse de Vulnérabilité** activée.

5. Choisissez les vulnérabilités du système que vous souhaitez vérifier régulièrement à l'aide des boutons correspondants.

Mises à jour critiques Windows

Vérifiez que votre système d'exploitation Windows dispose des dernières mises à jour de sécurité critiques de Microsoft.

Mises à jour d'applications

Vérifiez que les applications installées sur votre système sont à jour.Des applications non à jour peuvent être exploitées par des logiciels malveillants, rendant votre PC vulnérable aux attaques extérieures.

Mots de passe vulnérables

Vérifiez si les mots de passe des comptes Windows configurés sur le système sont faciles à deviner. Choisir des mots de passe difficiles à deviner rend difficile l'introduction dans votre système de pirates informatiques.Un mot de passe sécurisé est constitué d'une association de lettres majuscules, minuscules, de nombres et de caractères spéciaux (comme par exemple #, $ ou @).

Exécution automatique des supports amovibles

Vérifiez l'état de la fonctionnalité AutoRun de Windows.Cette fonctionnalité permet aux applications d'être automatiquement lancées à partir de CD, DVD, lecteurs USB ou autres périphériques externes.

Certains types de malwares utilisent la fonction AutoRun pour passer automatiquement des supports amovibles vers le PC. Nous vous recommandons donc de désactiver cette fonctionnalité Windows.



Note

Si vous désactivez la surveillance d'une certaine vulnérabilité, les problèmes qui y sont liés ne seront plus enregistrés dans la fenêtre Événements.

22. PARE-FEU

Le pare-feu protège votre ordinateur contre les tentatives de connexion non autorisées entrantes et sortantes, à la fois sur les réseaux locaux et sur Internet.Il fonctionne un peu comme un garde à votre porte - il surveille les tentatives de connexion et détermine celles à autoriser et à bloquer.

Le pare-feu Bitdefender utilise un ensemble de règles pour filtrer des données transmises vers et à partir de votre système. Les règles sont regroupées en 2 catégories :

Règles générales

Règles qui déterminent les protocoles sur lesquels la communication est autorisée.

Un ensemble de règles par défaut fournissant une protection optimale est utilisé. Vous pouvez éditer les règles en autorisant ou refusant des connections sur certains protocoles.

Règles d'applications

Règles déterminant comment chaque application peut accéder aux ressources réseau et à Internet.

Dans des conditions normales, Bitdefender crée automatiquement une règle lorsqu'une application essaie d'accéder à Internet. Vous pouvez également ajouter ou modifier manuellement des règles d'applications.

Si votre ordinateur fonctionne sous Windows Vista, Windows 7 ou Windows 8, Bitdefender attribue automatiquement un type de réseau à chaque connexion réseau qu'il détecte. En fonction du type de réseau, la protection pare-feu est définie pour le niveau approprié de chaque connexion.

Pour en savoir plus sur la configuration du pare-feu pour chaque type de réseau et sur comment modifier les paramètres réseau, veuillez vous reporter à *« Gérer les paramètres de connexion »* (p. 144).

22.1. Activer ou désactiver la protection pare-feu

Pour activer ou désactiver la protection pare-feu, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Pare-feu**.

4. Dans la fenêtre **Pare-feu**, cliquez sur le bouton Pare-feu.



Avertissement

La désactivation du pare-feu exposant votre ordinateur à des connexions non autorisées, il devrait s'agir d'une mesure temporaire. Réactivez le pare-feu dès que possible.

22.2. Gérer les règles de pare-feu

22.2.1. Règles générales

Quand des données sont transmises sur Internet, certains protocoles sont utilisés.

Les règles générales vous permettent de configurer les protocoles sur lesquels le trafic est autorisé. Par défaut, les règles générales ne s'affichent pas lorsque vous ouvrez le Pare-feu.Pour modifier les règles, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Pare-feu**.
4. Dans la fenêtre **Pare-feu**, sélectionnez l'onglet **Règles**.
5. Cochez la case **Afficher les règles générales** dans l'angle inférieur gauche de la fenêtre.

Les règles par défaut s'affichent. Pour éditer la priorité d'une règle, cliquez sur la flèche correspondante dans la colonne **Permission** et sélectionnez **Autoriser** ou **Refuser**.

DNS sur UDP / TCP

Autoriser ou refuser DNS sur UDP et TCP.

Par défaut, ce type de connexion est autorisé.

ICMP / ICMPv6 entrants

Autoriser ou refuser les messages ICMP / ICMPv6.

Les messages ICMP sont souvent utilisés par des pirates pour perpétrer des attaques contre les réseaux informatiques. Par défaut, ce type de connexion est refusé.

Envoi de courriels

Autoriser ou refuser l'envoi de courriels sur SMTP.

Par défaut, ce type de connexion est autorisé.

HTTP navigation Web

Autoriser ou refuser la navigation Web HTTP.

Par défaut, ce type de connexion est autorisé.

Connexions bureau à distance entrantes

Autoriser ou refuser l'accès à d'autres ordinateurs sur des connexions bureau à distance.

Par défaut, ce type de connexion est autorisé.

Trafic Windows Explorer sur HTTP / FTP

Autoriser ou refuser le trafic HTTP et FTP de Windows Explorer.

Par défaut, ce type de connexion est refusé.

22.2.2. Règles d'applications

Pour afficher et gérer les règles pare-feu contrôlant l'accès des applications aux ressources du réseau et à Internet, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Pare-feu**.
4. Dans la fenêtre **Pare-feu**, sélectionnez l'onglet **Règles**.

Vous pouvez consulter dans le tableau les programmes (c'est-à-dire les processus) pour lesquels des règles pare-feu ont été créées.Pour voir les règles créées pour une application spécifique, double-cliquez simplement dessus.

Les informations suivantes s'affichent pour chaque règle :

Nom - le nom du processus auquel les règles s'appliquent.

Types de Réseau - les types de processus et d'adaptateur réseau auxquels la règle s'applique.Des règles sont créées automatiquement pour filtrer l'accès réseau ou Internet via n'importe quel adaptateur.Les règles s'appliquent par défaut à tout réseau.Vous pouvez créer manuellement des règles ou éditer des règles existantes, afin de filtrer l'accès réseau ou

Internet d'une application via un adaptateur spécifique (par exemple un adaptateur réseau sans fil).

Protocole - le protocole IP auquel s'applique la règle.Les règles s'appliquent par défaut à tout protocole.

Permission - si l'application est autorisée ou non à se connecter au réseau ou à Internet dans certaines circonstances.

Pour gérer les règles, utilisez les boutons au-dessus du tableau :

Ajouter une règle - ouvre une fenêtre dans laquelle vous pouvez créer une nouvelle règle.

Supprimer la règle - supprime la règle sélectionnée.

Réinitialiser - ouvre une fenêtre où vous pouvez choisir de supprimer l'ensemble des règles existantes et de restaurer celles par défaut.

Ajouter / modifier des règles d'application

Pour ajouter ou modifier une règle d'application, cliquez sur le bouton **Ajouter une règle** au-dessus du tableau ou cliquez sur une règle existante.Une nouvelle fenêtre s'affiche. Procédez comme suit :

Chemin du programme. Cliquez sur **Parcourir** et sélectionnez l'application à laquelle s'applique la règle.

Adresse locale. Spécifiez l'adresse IP locale et le port auxquels s'applique la règle.Si vous avez plus d'un adaptateur réseau, vous pouvez décocher la case **Tous** et entrer une adresse IP spécifique.

Adresse distante. Spécifiez l'adresse IP distante et le port auxquels s'applique la règle.Pour filtrer le trafic entre votre ordinateur et un ordinateur spécifique, décochez la case **Tous** et entrer son adresse IP.

Version IP. Sélectionnez dans le menu la version du protocole IP (IPv4, IPv6 ou autre) à laquelle s'applique la règle.

Direction. Sélectionnez dans le menu la direction du trafic à laquelle s'applique la règle.

Direction	Description
Sortant	La règle s'applique seulement pour le trafic sortant.
Entrant	La règle s'applique seulement pour le trafic entrant.

Direction	Description
Tous les deux	La règle s'applique dans les deux directions.

Cliquez sur le lien **Plus d'options** pour d'autres actions :

Protocole. Sélectionnez dans le menu le protocole IP auquel s'applique la règle.

Si vous voulez que la règle s'applique à tous les protocoles, sélectionnez **Toutes**.

Si vous souhaitez que la règle s'applique au protocole TCP, sélectionnez **TCP**.

Si vous souhaitez que la règle s'applique au protocole UDP, sélectionnez **UDP**.

Si vous souhaitez que la règle s'applique à un protocole spécifique, saisissez le numéro affecté au protocole que vous souhaitez filtrer dans le champ vierge.



Note

Les numéros des protocoles IP sont attribués par l'IANA (Internet Assigned Numbers Authority, l'organisation de gestion de l'adressage IP sur Internet).Vous pouvez obtenir la liste complète des numéros de protocoles IP attribués à l'adresse http://www.iana.org/assignments/protocol-numbers.

Événements. En fonction du protocole sélectionné, choisissez les événements réseau auxquels la règle s'applique.Les événements suivants sont susceptibles d'être consignés :

Evénement	Description
Connexion	Échange préliminaire de messages standard, réalisé par les protocoles orientés connexion (tels que TCP) afin d'établir une connexion.Avec les protocoles orientés connexion, le trafic de données entre deux ordinateurs n'intervient qu'une fois qu'une connexion est établie.
Trafic	Flux de données entre deux ordinateurs.

Evénement	Description
Écoute	État dans lequel une application surveille le réseau, dans l'attente de l'établissement d'une connexion ou de la réception d'informations provenant d'une application de même niveau.

Réseau. Sélectionnez le type de réseau auquel s'applique la règle. Vous pouvez modifier le type de réseau en ouvrant le menu déroulant **Type de Réseau** et en sélectionnant l'un des types de réseau disponibles dans la liste.

Réseau	Description
De confiance	Désactiver le pare-feu pour l'adaptateur concerné.
Domicile/Pro.	Autoriser tout le trafic entre votre ordinateur et les ordinateurs du réseau local.
Public	Tout le trafic est filtré.
Non fiable	Bloquer complètement le trafic réseau et Internet via l'adaptateur respectif.

Permission. Sélectionnez l'une des permissions disponibles :

Permission	Description
Autoriser	L'application spécifiée se verra autoriser l'accès réseau/Internet dans les circonstances spécifiées.
Refuser	L'application spécifiée se verra refuser l'accès réseau/Internet dans les circonstances spécifiées.

22.3. Gérer les paramètres de connexion

Pour chaque connexion réseau vous pouvez configurer des zones de confiance et des zones non fiables.

Une zone de confiance est un périphérique en lequel vous avez entièrement confiance, comme un ordinateur ou une imprimante. Tout le trafic entre votre ordinateur et un périphérique de confiance est autorisé.Pour partager des

ressources avec des ordinateurs en particulier dans une réseau WiFi non sécurisé, ajoutez les comme étant des ordinateurs autorisés.

Une zone non fiable est un périphérique avec lequel vous n'autorisez aucune communication avec votre ordinateur.

Pour afficher et gérer les zones sur vos cartes réseau, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Pare-feu**.
4. Dans la fenêtre **Pare-feu**, sélectionnez l'onglet **Adaptateurs**.

Une nouvelle fenêtre apparaîtra indiquant les cartes réseau avec des connexions actives et les zones actuelles, le cas échéant.

Les informations suivantes s'affichent pour chaque zone :

Type de Réseau - le type de réseau auquel votre ordinateur est connecté.

Mode Furtif - détermine si vous pouvez être détecté par d'autres ordinateurs.

Pour configurer le mode furtif, sélectionnez l'option souhaitée dans le menu déroulant correspondant.

Option furtif	Description
Activé	Le mode Furtif est activé.Votre ordinateur n'est pas visible depuis le réseau local et Internet.
Désactivé	Le mode Furtif est désactivé.N'importe qui sur le réseau local ou sur Internet peut détecter votre ordinateur (via la commande ping).
Distant	Votre ordinateur ne peut pas être détecté depuis Internet.Les utilisateurs du réseau local peuvent voir (via la commande ping) et détecter votre ordinateur .

Générique - si des règles génériques sont appliquées à cette connexion.

Si l'adresse IP d'un adaptateur réseau est modifiée, Bitdefender modifie le type de réseau en conséquence.Si vous souhaitez conserver le même type de réseau, sélectionnez **Oui** dans le menu déroulant correspondant.

Ajouter / modifier des exceptions

Pour ajouter ou modifier une exception, cliquez sur le bouton **Exceptions Réseau** au-dessus du tableau.Une nouvelle fenêtre affichant les adresses IP des périphériques connectés au réseau s'affichera. Procédez comme suit :

1. Sélectionnez l'adresse IP de l'ordinateur que vous souhaitez ajouter, ou tapez une adresse ou une plage d'adresses dans la zone de texte prévue à cet effet.
2. Sélectionnez la permission :

   Autoriser - pour autoriser tout le trafic entre votre ordinateur et l'ordinateur sélectionné.

   Bloquer - permet de bloquer tout le trafic entre votre ordinateur et l'ordinateur sélectionné.
3. Cliquez sur le bouton + pour ajouter l'exception et fermez la fenêtre.

   Si vous souhaitez supprimer une IP, cliquez sur le bouton correspondant et fermez la fenêtre.

22.4. Configurer les paramètres avancés

Pour configurer les paramètres avancés du pare-feu, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Pare-feu.**
4. Dans la fenêtre **Pare-feu**, sélectionnez l'onglet **Configuration**.

Les fonctionnalités suivantes peuvent être activées ou désactivées.

Partage de Connexion Internet - active la prise en charge du partage de connexion Internet.



Note

Cette option n'active pas automatiquement le **Partage de connexion Internet** sur votre système, mais permet uniquement ce type de connexion si vous l'activez dans votre système d'exploitation.

Bloquer les analyses de port dans le réseau - détecte et bloque les démarches visant à détecter les ports ouverts.

Les analyses de ports sont fréquemment utilisées par les pirates pour découvrir des ports ouverts sur votre ordinateur.Ils peuvent alors s'introduire dans votre ordinateur, s'ils découvrent un port vulnérable ou moins sécurisé.

Surveiller les connexions Wi-Fi - si vous êtes connecté(e) à des réseaux sans fil, des informations s'affichent au sujet d'événements réseau spécifiques (par exemple lorsqu'un nouvel ordinateur rejoint le réseau).

23. DÉTECTION D'INTRUSION

La Détection d'Intrusion de Bitdefender surveille les activités du réseau et du système à la recherche d'activités malveillantes ou de violations de politique. Peut détecter et bloquer les tentatives de modification de fichiers système critiques, de fichiers Bitdefender ou d'entrées de registre, l'installation de pilotes malveillants et les attaques réalisées par injection de code (injection de DLL).

Pour configurer la Détection d'Intrusion, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Détection d'Intrusion**.
4. Pour activer la Détection d'Intrusion, cliquez sur le bouton correspondant.
5. Déplacez le curseur sur l'échelle pour choisir le degré d'analyse approprié.Reportez-vous à la description à droite de l'échelle pour choisir le niveau le plus adapté à vos besoins de sécurité.

Vous pouvez vérifier les applications détectées par la Détection d'Intrusion dans la fenêtre Événements.

Si vous avez confiance en certaines applications et ne souhaitez pas que la Détection d'Intrusion les analyse, vous pouvez ajouter des règles d'exclusion pour celles-ci. Pour exclure une application de l'analyse, suivez les étapes décrites dans la section *« Gérer les processus exclus »* (p. 115).



Note

Le fonctionnement de la Détection d'Intrusion est lié à celui d'Active Virus Control.Les règles d'exclusion de processus s'appliquent aux deux systèmes.

24. LA SÉCURITÉ SAFEPAY POUR LES TRANSACTIONS EN LIGNE

L'ordinateur devient rapidement indispensable pour les achats et les transactions bancaires. Payer vos factures, virer de l'argent, et acheter quasiment tout ce que vous pouvez imaginer n'a jamais été aussi rapide ni aussi simple.

Cela implique l'envoi sur Internet d'informations personnelles, de données de comptes et de cartes bancaires, de mots de passe et d'autres types d'informations confidentielles, en d'autres termes exactement le type d'informations qui intéressent tout particulièrement les cybercriminels. Les pirates ne sont pas avares d'efforts lorsqu'il s'agit de voler ces informations, et vous n'êtes donc jamais trop prudent pour ce qui est de la sécurisation des transactions en ligne.

Bitdefender Safepay™ est avant tout un navigateur protégé, un environnement sécurisé conçu pour assurer la confidentialité et la sécurité des opérations bancaires, achats en ligne et autres types de transactions sur Internet.

Pour une meilleure protection de la vie privée, Bitdefender Wallet est intégré à Bitdefender Safepay™ afin de protéger vos identifiants lorsque vous essayez d'accéder à des espaces en ligne confidentiels. Pour plus d'informations, consultez *« Protection Wallet de vos identifiants »* (p. 154).

Bitdefender Safepay™ dispose des fonctions suivantes :

- Il bloque l'accès à votre bureau et toute tentative de prise d'instantanés de votre écran.
- Il protège vos mots de passe confidentiels lorsque vous naviguez sur Internet avec Wallet.
- Il est accompagné d'un clavier virtuel, qui, lorsqu'il est utilisé, empêche les pirates de lire vos frappes au clavier.
- Il est complètement indépendant de vos autres navigateurs.
- Il contient une protection hotspot intégrée à utiliser lorsque votre ordinateur est connecté à des réseaux Wifi non sécurisés.
- Il supporte les marque-pages et vous permet de consulter vos sites bancaires et boutiques en ligne préférés.

Il ne se limite pas aux sites bancaires et boutiques en ligne. Tout site web peut être ouvert dans Bitdefender Safepay™.

24.1. Utiliser Bitdefender Safepay™

Par défaut, Bitdefender détecte que vous naviguez sur un site bancaire ou une boutique en ligne dans tout navigateur sur votre ordinateur et vous invite à le lancer dans Bitdefender Safepay™.

Pour accéder à l'interface principale de Bitdefender Safepay™, utilisez l'une des méthodes suivantes :

À partir de l'interface de Bitdefender :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur le bouton d'action **Safepay** à droite de la fenêtre.

À partir de Windows :

Dans **Windows XP**, **Windows Vista** et **Windows 7**:

1. Cliquez sur **Démarrer** et allez dans **Programmes**.
2. Cliquez sur **Bitdefender**.
3. Cliquez sur **Bitdefender Safepay™** ou sur le bouton d'action **Safepay** à droite de l'interface de Bitdefender.

Dans **Windows 8** :

Localisez Bitdefender Safepay™ dans l'écran d'accueil Windows (vous pouvez, par exemple, taper « Bitdefender Safepay™ » directement dans l'écran d'accueil) puis cliquez sur l'icône. Vous pouvez aussi cliquer sur le bouton d'action **Safepay** à droite de l'interface de Bitdefender.



Note

Si le plugin Adobe Flash Player n'est pas installé ou n'est pas à jour, un message Bitdefender apparaîtra. Cliquez sur le bouton correspondant pour poursuivre.
Une fois le processus d'installation terminé, vous pourrez rouvrir manuellement le navigateur Bitdefender Safepay™ pour poursuivre votre travail.

Si vous êtes habitués aux navigateurs web, vous n'aurez pas de problème pour utiliser Bitdefender Safepay™ - il ressemble et se comporte comme un navigateur standard :

saisissez les URL que vous souhaitez consulter dans la barre d'adresses.

ajoutez des onglets pour visiter plusieurs sites web dans la fenêtre de Bitdefender Safepay™ en cliquant sur .

naviguez d'une page à l'autre et actualisez les pages à l'aide de respectivement.

accédez aux paramètres de Bitdefender Safepay™ en cliquant sur .

protégez vos mots de passe avec Wallet en cliquant sur .

gérez vos marque-pages en cliquant sur à côté de la barre d'adresses.

ouvrez le clavier virtuel en cliquant sur .

24.2. Configurer les paramètres

Cliquez sur pour configurer les paramètres suivants :

Comportement général de Bitdefender Safepay™

Choisissez ce qui se passera lorsque vous accéderez à une boutique ou à un site bancaire en ligne dans un navigateur Web standard :

Ouvrir automatiquement dans Bitdefender Safepay™.

Faire en sorte que Bitdefender vous consulte pour l'action à chaque fois.

Ne jamais utiliser Bitdefender Safepay™ pour les pages consultées dans un navigateur standard.

Liste des domaines

Choisissez comment Bitdefender Safepay™ se comportera lorsque vous consulterez les sites web de certains domaines dans votre navigateur Web standard en les ajoutant à la liste de domaines et en sélectionnant son comportement pour chacun d'entre eux :

Ouvrir automatiquement dans Bitdefender Safepay™.

Faire en sorte que Bitdefender vous consulte pour l'action à chaque fois.

Ne jamais utiliser Bitdefender Safepay™ lors de la consultation d'une page de ce domaine dans un navigateur standard.

Bloquer les pop-up

Vous pouvez choisir de bloquer les fenêtres pop-up en cliquant sur le bouton correspondant.

Vous pouvez également créer une liste de sites web dont vous autorisez les fenêtres pop-up. La liste ne doit contenir que des sites Web de confiance.

Pour ajouter un site à la liste, saisissez son adresse dans le champ correspond et cliquez sur **Ajouter un domaine**.

Pour supprimer un site Web de la liste, sélectionnez-le dans la liste et cliquez sur le lien **Supprimer**.

24.3. Gérer les marque-pages

Si vous avez désactivé la détection automatique de certains ou de tous les sites web, ou si Bitdefender ne détecte simplement pas certains sites web, vous pouvez ajouter des marque-pages à Bitdefender Safepay™ afin de pouvoir lancer facilement vos sites web favoris à l'avenir.

Suivez ces étapes pour ajouter une URL aux marque-pages de Bitdefender Safepay™ :

1. Cliquez sur à côté de la barre d'adresses pour ouvrir la page Marque-pages.



Note
La page Marque-pages s'ouvre par défaut lorsque vous lancez Bitdefender Safepay™.

2. Cliquez sur le bouton **+** pour ajouter un nouveau marque-pages.
3. Indiquez l'URL et le titre du marque-pages et cliquez sur **Créer**. L'URL est également ajoutée à la Liste de domaines sur la page paramètres.

24.4. Protection hotspot pour les réseaux non sécurisés

Lorsque vous utilisez Bitdefender Safepay™ en étant connecté à des réseaux Wifi non sécurisés (par exemple, à un point d'accès public), un niveau de sécurité supplémentaire est fourni par la fonctionnalité Protection Hotspot. Ce service chiffre la communication Internet sur des connexions non sécurisées, vous aidant à assurer la protection de votre vie privée quel que soit le réseau auquel vous êtes connecté.

Les prérequis suivants doivent être remplis pour que la protection hotspot fonctionne :

- Vous êtes connecté à un compte MyBitdefender depuis Bitdefender Internet Security 2015.
- Votre ordinateur est connecté à un réseau non sécurisé.

Une fois les prérequis remplis, Bitdefender vous demandera automatiquement d'utiliser la connexion sécurisée lorsque vous ouvrirez Bitdefender Safepay™. Saisissez simplement vos identifiants MyBitdefender lorsque vous y êtes invité.

La connexion sécurisée sera initialisée et un message s'affichera dans la fenêtre Bitdefender Safepay™ lorsque la connexion sera établie. Le symbole apparaît en face de l'URL dans la barre d'adresses pour vous aider à identifier facilement les connexions sécurisées.

Pour améliorer votre expérience de navigation visuellement, vous pouvez choisir d'activer les plugins **Adobe Flash** et **Java** en cliquant sur **Afficher les paramètres avancés**.

Vous aurez peut-être besoin de confirmer l'action.

25. PROTECTION WALLET DE VOS IDENTIFIANTS

Nous utilisons l'ordinateur pour effectuer des achats en ligne ou payer nos factures, pour nous connecter à des plateformes de réseaux sociaux ou à des applications de messagerie instantanée.

Mais comme chacun le sait, ce n'est pas toujours facile de se souvenir des mots de passe !

Et si nous ne sommes pas prudents sur Internet, nos informations confidentielles telles que notre adresse courriel, nos identifiants de messagerie instantanée ou les données de notre carte bancaire peuvent être compromises.

Noter vos mots de passe ou vos données confidentielles sur une feuille de papier ou dans votre ordinateur peut être dangereux car cela les rend accessibles à des personnes qui souhaitent les dérober et les utiliser. Et vous souvenir de tous les mots de passe que vous avez définis pour vos comptes en ligne ou pour vos sites Web préférés n'est pas une tâche facile.

Y a-t-il un moyen de nous garantir de trouver nos mots de passe au moment où nous en avons besoin ? Et pouvons-nous être sûrs que nos mots de passe confidentiels sont en sécurité ?

Wallet est le gestionnaire de mots de passe qui vous aide à conserver vos mots de passe, protège votre vie privée et vous offre une expérience de navigation sécurisée.

En utilisant un mot de passe principal unique pour accéder à vos identifiants, Wallet vous permet de conserver facilement vos mots de passe en sécurité.

Pour fournir la meilleure protection possible à vos activités en ligne, Wallet est intégré à Bitdefender Safepay™ et offre une solution intégrée pour répondre aux différentes façons dont vos données confidentielles peuvent être compromises.

Wallet protège les informations confidentielles suivantes :

- Des informations personnelles, telles que l'adresse courriel ou le numéro de téléphone
- Les identifiants de connexion aux sites Web
- Les informations bancaires sur les comptes et les numéros de carte
- Les données permettant d'accéder aux comptes de messagerie

- Les mots de passe des applications
- Les mots de passe des réseaux Wifi

25.1. Configurer Wallet

Une fois l'installation terminée, lorsque vous ouvrirez votre navigateur, une fenêtre contextuelle vous indiquera que vous pouvez utiliser Wallet pour faciliter votre navigation sur Internet.

Cliquez sur **Explorer** pour lancer l'assistant de configuration de Wallet. Suivez l'assistant pour terminer le processus de configuration.

Deux tâches peuvent être réalisées au cours de cette étape :

- Créer une nouvelle base de données Wallet pour protéger vos mots de passe.

  Lors de la configuration, vous serez invité à protéger votre Wallet avec un mot de passe principal. Le mot de passe doit être sécurisé et contenir au moins 7 caractères.

  Pour créer un mot de passe sécurisé, utilisez au moins un chiffre ou un symbole et une majuscule. Une fois que vous aurez défini un mot de passe, toute personne essayant d'accéder au Wallet devra indiquer ce mot de passe.

  À la fin de la configuration, les paramètres suivants de Wallet sont activés par défaut :

  - **Enregistrer automatiquement les identifiants dans Wallet**.
  - **Me demander mon mot de passe principal lorsque je me connecte à mon ordinateur**.
  - **Verrouiller automatiquement Wallet lorsque mon PC n'est pas utilisé**.

- Importez une base de données existante si vous avez déjà utilisé Wallet sur votre système.

Exporter la base de données du Wallet

Pour exporter la base de données de votre Wallet, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Vie privée**.
3. Dans le module **Wallet**, sélectionnez **Exporter Wallet**.

4. Suivez ces étapes pour exporter la base de données du Wallet vers votre système.

Créer une nouvelle base de données du Wallet

Pour créer une nouvelle base de données du Wallet, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Vie privée**.
3. Dans le module **Wallet**, sélectionnez **Créer un Wallet**.
4. Une fenêtre d'avertissement vous informera que les données actuellement stockées dans le Wallet seront supprimées. Cliquez sur **Oui** pour supprimer une base de données existante et continuer avec l'assistant. Pour quitter l'assistant, cliquez sur **Non**.

Gérer les identifiants de votre Wallet

Pour gérer vos mots de passe, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Vie privée**.
3. Dans le module **Wallet**, sélectionnez **Ouvrir Wallet**.

Une nouvelle fenêtre s'affiche. Sélectionnez la catégorie souhaitée dans la partie supérieure de la fenêtre :

Identité

Sites Web

Banques

Clients email

Applications

Réseaux Wifi

Ajouter/ modifier les identifiants

Pour ajouter un nouveau mot de passe, choisissez la catégorie souhaitée en haut, cliquez sur **+ Ajouter un élément**, insérez les informations dans les champs correspondants et cliquez sur le bouton Enregistrer.

Pour éditer un objet de la liste, sélectionnez le et cliquez sur le bouton **Editer**.

Pour quitter, cliquez sur **Annuler**.

Pour supprimer une entrée, sélectionnez-la, cliquez sur le bouton **Modifier** et sélectionnez **Supprimer**.

25.2. Activer ou désactiver la protection du Wallet

Pour activer ou désactiver la protection du Wallet, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Vie privée**.
3. Cliquez sur le module **Wallet**.
4. Dans la fenêtre **Wallet**, cliquez sur le bouton pour activer ou désactiver **Wallet**.

25.3. Gérer les paramètres du Wallet

Pour configurer le mot de passe principal en détail, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Vie privée**.
3. Cliquez sur le module **Wallet**.
4. Dans la fenêtre **Wallet**, sélectionnez l'onglet **Mot de passe principal**.

Voici les options proposées :

Me demander mon mot de passe principal lorsque je me connecte à mon PC - vous devrez indiquer votre mot de passe principal lorsque vous accéderez à l'ordinateur.

Me demander mon mot de passe principal lorsque j'ouvre mes navigateurs et applications - vous devrez indiquer votre mot de passe principal lorsque vous accéderez à un navigateur ou à une application.

Verrouiller automatiquement Wallet lorsque mon PC n'est pas utilisé - vous devrez saisir votre mot de passe principal lorsque vous utiliserez votre ordinateur après 15 minutes d'inactivité.



Important
N'oubliez pas votre mot de passe principal ou conservez-le en lieu sûr. Si vous oubliez le mot de passe, vous devrez réinstaller le programme ou contacter le support Bitdefender.

Améliorer votre expérience

Pour sélectionner les navigateurs ou les applications où vous souhaitez intégrer le Wallet, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Vie privée**.
3. Cliquez sur le module **Wallet**.
4. Dans la fenêtre **Wallet**, sélectionnez l'onglet **Applications améliorées**.

   Cochez une application pour utiliser le Wallet et améliorer votre expérience :

   Internet Explorer

   Mozilla Firefox

   Google Chrome

   Safepay

   Yahoo! Messenger

   Skype

Configurer la saisie automatique

La fonctionnalité Saisie automatique vous permet d'accéder facilement à vos sites web préférés ou de vous connecter à vos comptes en ligne. Lorsque vous saisissez vos informations d'identification et données personnelles dans votre navigateur web pour la première fois, celles-ci sont automatiquement conservées en toute sécurité dans Wallet.

Pour configurer les paramètres de la **Saisie automatique**, les étapes sont les suivantes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Vie privée**.
3. Cliquez sur le module **Wallet**.

4. Dans la fenêtre **Wallet**, sélectionnez l'onglet **Paramètres de la saisie automatique**.
5. Configurez les options suivantes :

    Saisir automatiquement les identifiants de connexion:

    Saisir automatiquement les identifiants de connexion à chaque fois - les identifiants de connexion sont insérés automatiquement dans le navigateur.

    Me laisser choisir quand je souhaite que mes identifiants de connexion soient saisis automatiquement - vous pouvez choisir quand les identifiants seront saisis automatiquement dans le navigateur.

    Configurer la façon dont Wallet sécurise vos identifiants:

    Enregistrer automatiquement les identifiants dans Wallet - les identifiants de connexion et autres informations identifiables telles que vos données personnelles et bancaires sont automatiquement enregistrées et mises à jour dans le Wallet.

    Me demander à chaque fois - on vous demandera à chaque fois si vous souhaitez ajouter vos identifiants au Wallet.

    Ne pas enregistrer, je mettrai les informations à jour manuellement - les identifiants peuvent être ajoutés uniquement manuellement dans le Wallet.

    Compléter automatiquement les formulaires:

    Me demander mes options de saisie lorsque je consulte une page contenant des formulaires - une fenêtre avec les options de remplissage apparaîtra à chaque fois que Bitdefender détectera que vous souhaitez effectuer un paiement en ligne ou vous connecter.

Gérer les informations de Wallet à partir de votre navigateur

Vous pouvez facilement gérer Wallet directement à partir de votre navigateur afin d'avoir toutes vos données importantes à portée de main. L'add-on Wallet est compatible avec les navigateurs suivants : Google Chrome, Internet Explorer et Mozilla Firefox et est également intégré à Safepay.

Pour accéder à l'extension Wallet, ouvrez votre navigateur web, autorisez l'installation de l'add-on et cliquez sur l'icône de la barre d'outils.

L'extension Wallet présente les options suivantes :

Ouvrir Wallet - ouvre le Wallet.

Verrouiller Wallet - verrouille le Wallet.

Sites web - ouvre un sous-menu avec tous les identifiants de sites web contenus dans Wallet. Cliquez sur **Ajouter un site web** pour ajouter de nouveaux sites web à la liste.

Remplir les formulaires - ouvre un sous-menu contenant les informations que vous avez ajoutées pour une catégorie spécifique. Vous pouvez ajouter ici de nouvelles données à votre Wallet.

Configuration - ouvre la fenêtre des paramètres de Wallet.

Signaler un problème - permet de signaler tout problème rencontré avec Bitdefender Wallet.

26. CONTRÔLE PARENTAL

Le module de contrôle parental vous permet de contrôler l'accès à Internet et à des applications spécifiques pour chaque utilisateur disposant d'un compte utilisateur sur le système.

Une fois le contrôle parental configuré, il est facile pour vous de connaître les activités de votre enfant sur l'ordinateur.

Il vous suffit d'un ordinateur avec accès Internet et d'un navigateur Web.

Vous pouvez configurer le contrôle parental pour bloquer :

- aux pages Web indésirables.
- l'accès à Internet, pour des périodes bien définies (l'heure des devoirs, par exemple).
- les applications comme les jeux, les logiciels de clavardage, les programmes de partage de fichiers et autres.
- les messages instantanés envoyés par des contacts de messagerie instantanée autres que ceux autorisés.

Vérifiez les activités de vos enfants et modifiez les paramètres du contrôle parental à l'aide de MyBitdefender depuis tout ordinateur ou appareil mobile connecté à Internet.

26.1. Accéder au tableau de bord du contrôle parental

Le tableau de bord du contrôle parental est organisé en modules qui vous permettent de surveiller les activités de l'enfant sur l'ordinateur.

Bitdefender vous permet de contrôler l'accès de vos enfants à Internet et à certaines applications. Il vous permet également de surveiller l'activité de leur compte Facebook.

Bitdefender vous permet d'accéder aux paramètres du Contrôle Parental depuis un compte MyBitdefender sur tout ordinateur ou appareil mobile connecté à Internet.

Accédez à votre compte en ligne :

Sur tout appareil avec un accès à Internet :

1. Ouvrez un navigateur Web.
2. Allez à :https://my.bitdefender.com

3. Connectez-vous à votre compte à l'aide de votre nom d'utilisateur et de votre mot de passe.
4. Cliquez sur **Contrôle Parental** pour accéder au tableau de bord.

Depuis votre interface Bitdefender :

1. Assurez-vous d'être connecté à l'ordinateur en utilisant un compte administrateur. Seuls les utilisateurs ayant des droits d'administrateur sur le système peuvent avoir accès et configurer le contrôle parental.
2. Ouvrez la fenêtre de Bitdefender.
3. Accédez au panneau **Vie privée**.
4. Sous le module **Contrôle Parental**, sélectionnez **Configurer**.

   Vérifiez que vous êtes connecté à votre compte MyBitdefender.
5. Le tableau de bord du contrôle parental s'ouvrira dans une nouvelle fenêtre. Vous pouvez vérifier et configurer ici les paramètres du contrôle parental de chaque compte utilisateur Windows.

26.2. Ajouter le profil de votre enfant

Avant de configurer le contrôle parental, créez un compte utilisateur Windows pour chaque enfant. Cela vous permettra de connaître exactement les activités de chacun d'entre eux sur l'ordinateur. Nous vous recommandons de créer des comptes utilisateur limités (standard) afin qu'ils ne puissent pas modifier les paramètres du contrôle parental. Pour plus d'informations, consultez *« Comment créer des comptes utilisateurs Windows ? »* (p. 70).

Pour ajouter le profil de votre enfant au contrôle parental :

1. Accédez au tableau de bord du Contrôle Parental depuis votre compte MyBitdefender.
2. Cliquez sur **Ajouter un enfant** sur le menu de gauche.
3. Indiquez le nom et l'âge de l'enfant dans les champs correspondants. Si vous précisez l'âge de l'enfant, des paramètres considérés comme étant adaptés à cet âge seront automatiquement chargés, basés sur les normes de développement de l'enfant.
4. Vous pouvez voir ci-dessous les appareils liés à votre compte MyBitdefender.
5. Sélectionnez l'ordinateur et le compte Windows de votre enfant.

6. Cliquez sur **Créer un profil**.

   L'ordinateur et le compte Windows de votre enfant sont désormais liés à votre compte MyBitdefender.

26.2.1. Installation du Contrôle Parental sur l'appareil Android

Pour installer le Contrôle Parental sur l'appareil mobile de votre enfant, procédez comme suit :

1. Accédez au tableau de bord du Contrôle Parental depuis votre compte MyBitdefender.
2. Cliquez sur **Ajouter un enfant** sur le menu de gauche.
3. Indiquez le nom et l'âge de l'enfant dans les champs correspondants. Si vous précisez l'âge de l'enfant, des paramètres considérés comme étant adaptés à cet âge seront automatiquement chargés, basés sur les normes de développement de l'enfant.
4. Cliquez sur **Installer sur un nouvel appareil** pour poursuivre.
5. Une nouvelle fenêtre s'affiche. Sélectionnez **Google Play** dans la liste.
6. Pour télécharger et installer le Contrôle Parental sur l'appareil, cliquez sur le bouton **Installer**.
7. Sélectionnez l'appareil où vous souhaitez installer l'application.
8. Cliquez sur **Installer** pour poursuivre.

   Patientez pendant que l'application s'installe sur l'appareil. Vérifiez que l'appareil de l'enfant est connecté à Internet.
9. À la fin de l'installation, vous serez invité à donner les droits administrateur de l'application sur l'appareil.
10. Appuyez sur **Accepter** pour terminer l'installation.

Lier le Contrôle Parental à MyBitdefender

Pour surveiller l'activité en ligne de votre enfant, vous devez lier l'appareil de l'enfant à votre compte MyBitdefender en vous connectant au compte à partir de l'application.

Pour associer l'appareil à votre compte MyBitdefender, suivez ces étapes :

1. Indiquez le nom d'utilisateur et le mot de passe de votre compte MyBitdefender.

   Si vous n'avez pas de compte, choisissez de créer un nouveau compte à l'aide du bouton correspondant.

   Note
   Vous pouvez également indiquer un nom pour votre appareil. Associer plus d'un appareil à votre compte vous aidera à identifier les appareils plus facilement.

2. Appuyez sur **Connexion**.

   L'appareil de votre enfant est désormais lié à votre compte MyBitdefender et vous pouvez commencer à surveiller ses activités sur Internet.

26.2.2. Surveiller les activités de l'enfant

Bitdefender vous aide à surveiller l'activité de vos enfants sur Internet.

Vous pouvez de cette façon toujours savoir exactement quels sites Web ils ont consultés, quelles applications ils ont utilisées et les activités bloquées par le contrôle parental.

Les rapports contiennent des informations détaillées pour chaque événement, comme :

L'état de l'événement.

Le nom du site Web bloqué.

Le nom de l'application bloquée.

Le nom de l'appareil.

La date et l'heure auxquelles l'événement a eu lieu.

Les actions appliquées par Bitdefender.

Pour surveiller le trafic Internet, les applications auxquelles a accédé votre enfant et ses activités, procédez comme suit :

1. Accédez au tableau de bord du contrôle parental depuis votre compte MyBitdefender.
2. Cliquez sur pour accéder à la fenêtre d'activité du module correspondant.

26.2.3. Configurer les paramètres généraux

Rapports d'activité

Lorsque le contrôle parental est activé, les activités de vos enfants sont enregistrées par défaut.

Pour recevoir des notifications par courriel, procédez comme suit :

1. Accédez au tableau de bord du contrôle parental depuis votre compte MyBitdefender.
2. Cliquez sur l'icône **Paramètres généraux** dans l'angle supérieur droit.
3. Activez l'option correspondante pour recevoir les rapports d'activité.
4. Saisissez l'adresse courriel pour recevoir les notifications par courriel.
5. Ajustez la fréquence en sélectionnant : quotidienne, hebdomadaire ou mensuelle.
6. Recevez des notifications par courriel pour les éléments suivants :

   Sites Web bloqués

   Applications bloquées

   Contact de messagerie instantanée bloqué

   SMS d'un contact bloqué

   Appel reçu d'un numéro de téléphone bloqué

   Désinstallation de l'application de contrôle parental pour Facebook
7. Cliquez sur **Enregistrer**.

Informations sur le compte

Consultez la zone **Infos du compte**. Vous pouvez voir l'état de l'enregistrement, la clé de la licence actuelle et la date d'expiration.

Activez l'option pour mettre à jour les agents installés sur vos appareils et ajustez la fréquence en sélectionnant : quotidienne, hebdomadaire ou mensuelle.



Note
Cochez la case correspondante pour masquer l'écran d'accueil.

26.3. Configurer le contrôle parental

Le tableau de bord du contrôle parental vous permet de gérer directement les modules du contrôle parental.

Chaque module contient les éléments suivants : le nom du module, un message d'état, l'icône du module et un bouton qui vous permet d'effectuer d'importantes tâches liées au module.

Cliquez sur un onglet pour configurer la fonction de contrôle parental correspondante pour l'ordinateur :

Web - permet de filtrer la navigation Web et de définir des restrictions horaires pour l'accès à Internet.

Applications - permet de bloquer ou de limiter l'accès à certaines applications.

Facebook - permet de protéger le compte Facebook de votre enfant.

Messagerie Instantanée - permet d'autoriser ou de bloquer les conversations avec certains contacts de messagerie instantanée.

Vous pouvez accéder aux modules suivants pour surveiller l'activité de votre enfant sur l'appareil mobile :

Localisation - permet de situer l'appareil de votre enfant sur Google Maps.

SMS - pour bloquer les messages de texte provenant d'un numéro de téléphone spécifique.

Appels - pour bloquer les appels d'un numéro de téléphone, entrants et sortants.

26.3.1. Contrôle Web

Le Contrôle Web vous aide à bloquer les sites web au contenu inapproprié et à définir des restrictions horaires pour l'accès à Internet.

Pour configurer le Contrôle Web pour un compte utilisateur spécifique :

1. Cliquez sur le panneau **Web** pour accéder à la fenêtre **Activité Web**.
2. Utilisez le bouton pour activer l'**Activité Web**.

Autoriser ou bloquer un site Web

Utilisez la fenêtre **Activité Web** pour voir toutes les pages Web auxquelles votre enfant a accédé.

Pour bloquer l'accès à un site Web, procédez comme suit :

1. Cliquez sur le bouton **Liste noire/Liste blanche**.
2. Indiquez le site Web dans le champ correspondant.
3. Cliquez sur **Bloquer** pour ajouter le site Web à la liste.
4. Si vous changez d'avis, sélectionnez le site Web et cliquez sur le bouton **Supprimer** correspondant.

Pour autoriser l'accès à un site Web bloqué, procédez comme suit :

1. Cliquez sur le bouton **Liste noire/Liste blanche**.
2. Indiquez le site Web dans le champ correspondant.
3. Cliquez sur **Autoriser** pour ajouter le site Web à la liste.
4. Si vous changez d'avis, sélectionnez le site Web et cliquez sur le bouton **Supprimer** correspondant.

Pour limiter l'accès Internet à un site web par heure, suivez ces étapes :

1. Accédez à la fenêtre Web, Liste noire / Liste blanche où vous pouvez voir les pages web bloquées/autorisées.
2. Sous Permission, cliquez sur Bloqué (ou Autorisé) et sélectionnez Planifier dans le menu déroulant.
3. Sélectionnez dans la grille les intervalles pendant lesquels l'accès est autorisé ou bloqué. Vous pouvez cliquer sur des cellules individuelles pour choisir des heures ou cliquer et faire glisser la souris sur plusieurs cellules pour bloquer de plus longues périodes.

   Cliquez sur le bouton **Sauvegarder**.

Contrôle par mots-clés

Le contrôle par mots-clés vous aide à bloquer l'accès des utilisateurs aux messages instantanés et aux pages Web contenant certains mots. Le contrôle par mots-clés vous permet d'empêcher que vos enfants ne voient des mots ou des expressions inappropriés lorsqu'ils sont en ligne. En outre, vous pouvez faire en sorte qu'aucune information personnelle (adresse de

domicile ou téléphone par exemple) ne soit fournie aux personnes rencontrées sur Internet.

Pour configurer le contrôle par mots-clés pour un compte utilisateur spécifique, procédez comme suit :

1. Cliquez sur le bouton **Mots-clés**.
2. Indiquez le mot-clé dans le champ correspondant.
3. Cliquez sur **Bloquer** pour ajouter le mot à la liste des mots-clés interdits. Si vous changez d'avis, cliquez sur le bouton **Supprimer** correspondant.

Filtrage par catégories

Le Filtrage par catégories filtre de façon dynamique l'accès aux sites Web en fonction de leur contenu. Lorsque vous définissez l'âge de votre enfant, le filtre est automatiquement configuré pour bloquer les catégories de sites Web considérées comme inappropriées à l'âge de votre enfant. Cette configuration convient à la plupart des cas.

Si vous souhaitez mieux contrôler le contenu Internet auquel votre enfant est exposé, vous pouvez choisir les catégories de sites Web à bloquer avec le filtrage par catégories.

Pour configurer en détail l'accès aux paramètres du filtrage par catégories pour un compte utilisateur spécifique, procédez comme suit :

1. Cliquez sur le bouton **Catégories**.
2. Vous pouvez vérifier les catégories Web bloquées/restreintes automatiquement pour les âges sélectionnés. Si vous n'êtes pas satisfait des paramètres par défaut, vous pouvez les configurer selon vos besoins.
3. Cliquez sur **Enregistrer**. Si vous changez d'avis, cliquez sur le bouton **Réinitialiser** pour utiliser le niveau de protection par défaut en fonction de l'âge de votre enfant.

Limiter l'accès à Internet en fonction de l'heure

Vous pouvez spécifier quand votre enfant est autorisé à accéder à Internet à l'aide de l'option **Planification** dans la fenêtre **Activité Web**.

Pour configurer en détail l'accès à Internet pour un compte utilisateur spécifique, procédez comme suit :

1. Cliquez sur le bouton **Planifier**.

2. Sélectionnez dans la grille les intervalles de temps pendant lesquels l’accès à Internet est bloqué. Vous pouvez cliquer sur des cellules individuelles pour choisir des heures ou cliquer et faire glisser la souris sur plusieurs cellules pour bloquer de plus longues périodes.
3. Cliquez sur le bouton **Sauvegarder**.

26.3.2. Contrôle des applications

Le contrôle des applications vous aide à bloquer l'exécution de toute application. Les jeux, logiciels multimédias et services de messagerie, ainsi que d’autres catégories de logiciels et de malwares peuvent être bloqués de cette manière.

Pour configurer le contrôle des applications pour un compte utilisateur spécifique, procédez comme suit :

1. Cliquez sur le panneau **Applications** pour accéder à la fenêtre **Activité des Applications**.
2. Utilisez le bouton pour activer l'**Activité des Applications**.
3. Cliquez sur le bouton **Liste noire**.
4. Saisissez le nom de l'application :

   Pour bloquer une application mobile, sélectionnez les applications que vous souhaitez bloquer depuis la liste des **Applications autorisées**.

   Pour bloquer un programme Windows, ajoutez le fichier exécutable du programme que vous souhaitez bloquer (.exe).
5. Cliquez sur **Bloquer** pour ajouter l’application à la liste des **Applications bloquées** ou sur **Autoriser** pour ajouter l'application à la liste des **Applications autorisées**.

26.3.3. Protection Facebook

Le contrôle parental surveille le compte Facebook de votre enfant et signale ses principales activités.

Ces activités en ligne sont vérifiées et vous êtes averti si elles constituent une menace pour la confidentialité de votre compte.

Les éléments surveillés du compte en ligne comprennent :

- le nombre d’amis

- les commentaires de l'enfant ou de ses amis sur ses photos ou publications
- messages
- les publications du mur
- les photos et vidéos téléchargées
- les paramètres de confidentialité du compte

Pour configurer la protection Facebook pour un compte utilisateur spécifique :

1. Cliquez sur **Connecter le profil de l'enfant** dans le panneau **Facebook**.
2. Pour protéger le compte Facebook de l'enfant, installez l'application à l'aide du lien correspondant.



Note
Vous aurez besoin des identifiants du profil Facebook de votre enfant pour installer l'application.

Pour cesser de surveiller le compte Facebook, utilisez le bouton **Dissocier le compte** en haut.

26.3.4. Contrôle des messageries instantanées

Le contrôle des messageries instantanées (MI) vous permet de spécifier les contacts de MI avec lesquels vos enfants sont autorisés à discuter et de bloquer l'accès aux messages instantanés contenant certains mots.



Note
Le contrôle des MI est disponible uniquement pour Yahoo! Messenger.

Pour configurer le contrôle des Messageries Instantanées pour un compte utilisateur spécifique, procédez comme suit :

1. Cliquez sur le panneau **Messagerie instantanée** pour accéder à la fenêtre **Activité messageries instantanées**.
2. Utilisez le bouton pour activer l'**activité messageries instantanées**.

   Limitez l'accès à la **messagerie instantanée** à l'aide de l'une des options disponibles :

   - Le bouton **Liste noire** permet de saisir l'adresse courriel associée à l'ID de messagerie instantanée.

Le bouton **Mots-clés** pour bloquer l'accès aux messages instantanés contenant certains mots.

26.3.5. Emplacement

Afficher l'emplacement actuel de l'appareil sur Google Maps. Son emplacement est actualisé toutes les 5 secondes, afin que vous puissiez le suivre en cas de déplacement.

La précision de la localisation dépend de la façon dont Bitdefender est capable de la déterminer :

Si le GPS est activé sur l'appareil, son emplacement peut être déterminé à quelques mètres près tant qu'il est à portée des satellites GPS (c'est-à-dire, à l'extérieur).

Si l'appareil est à l'intérieur, il peut être localisé avec une précision d'une dizaine de mètres si le Wifi est activé et si des réseaux sans fil sont à sa portée.

Sinon, la localisation sera déterminée à l'aide des informations du réseau mobile, qui fournit une précision de pas plus de quelques centaines de mètres.



Note
Pour que la **Localisation** soit précise, vérifiez que vous avez activé le GPS, le Wifi ou la connexion au réseau mobile sur l'appareil mobile.

26.3.6. Contrôle des messages textes

Le contrôle des messages textes vous permet de bloquer les textes provenant d'un numéro de téléphone spécifique.

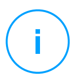
Pour bloquer les textes provenant d'un numéro de téléphone spécifique, procédez comme suit :

1. Cliquez sur le panneau **SMS** pour accéder à la fenêtre **Activité SMS**.
2. Utilisez le bouton pour activer **Activité SMS**.
3. Cliquez sur le bouton **Liste noire**.
4. Ajoutez un numéro de téléphone dans le champ correspondant.

5. Cliquez sur **Bloquer** pour ajouter le numéro de téléphone à la liste noire. Le numéro de téléphone sera ajouté à la liste des numéros de téléphone bloqués.

Pour autoriser les textes provenant d'un numéro de téléphone bloqué, procédez comme suit :

1. Cliquez sur le bouton **Liste noire** en haut.
2. Sélectionnez le numéro de téléphone dans la liste.
3. Cliquez sur **Supprimer**. Le numéro de téléphone sera retiré de la liste des numéros de téléphone bloqués.



Note
Veillez à utiliser le code du pays lorsque vous ajoutez le numéro de téléphone à la liste.

26.3.7. Contrôle des numéros de téléphone

Le contrôle des numéros de téléphone vous aide à arrêter d'appeler un numéro spécifique ou à recevoir des appels de celui-ci.

Pour bloquer l'envoi ou la réception d'appels associés à un numéro de téléphone, procédez comme suit :

1. Cliquez sur le panneau **Appels** pour accéder à la fenêtre **Activité des Appels**.
2. Utilisez le bouton pour activer l'**Activité des appels**.
3. Cliquez sur le bouton **Liste noire**.
4. Ajoutez un numéro de téléphone dans le champ correspondant.
5. Cliquez sur **Bloquer** pour ajouter le numéro de téléphone à la liste noire. Le numéro de téléphone sera ajouté à la liste des numéros de téléphone bloqués.

Pour autoriser les appels vers un numéro de téléphone bloqué, procédez comme suit :

1. Cliquez sur le bouton **Liste noire** en haut.
2. Sélectionnez le numéro de téléphone dans la liste.
3. Cliquez sur **Supprimer**. Le numéro de téléphone sera retiré de la liste des numéros de téléphone bloqués.



Note
Veillez à utiliser le code du pays lorsque vous ajoutez le numéro de téléphone à la liste.

27. PROTECTION SAFEGO POUR FACEBOOK

Vous faites confiance à vos amis en ligne, mais faites-vous confiance à leurs ordinateurs ?Utilisez la protection Facebook afin de mettre votre compte et vos amis à l'abri des menaces en ligne.

Safego est une application Bitdefender développée pour assurer la sécurité de votre compte Facebook.Son rôle consiste à analyser les liens que vous recevez de la part de vos amis et à surveiller les paramètres de confidentialité de votre compte.



Note
Un compte MyBitdefender est nécessaire pour utiliser cette fonctionnalité. Pour plus d'informations, consultez « *Compte MyBitdefender* » (p. 41).

Les principales fonctionnalités disponibles pour votre compte Facebook sont les suivantes :

analyse automatiquement les publications de votre fil d'actualité à la recherche de liens malveillants.

protège votre compte des menaces en ligne.

Lorsqu'une publication ou un commentaire sera détecté comme étant du spam, une tentative de phishing ou un malware, vous recevrez un message d'avertissement.

avertit vos amis des liens suspects publiés sur leurs fils d'actualité.

vous aide à construire un réseau d'amis sûr à l'aide de la fonctionnalité **Friend'O'Meter**.

vérifier l'état de sécurité du système grâce à Bitdefender QuickScan.

Pour accéder à Safego pour Facebook, procédez comme suit :

À partir de l'interface de Bitdefender :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Outils**.
3. Sous le module **Safego**, sélectionnez **Activer pour Facebook**.

   Vous serez dirigé vers votre compte.
4. Utilisez vos informations de connexion Facebook pour vous connecter à l'application Safego.

5. Autoriser Safego à accéder à votre compte Facebook.

Si Safego a déjà été activé, vous pouvez accéder à des statistiques sur son activité en cliquant sur **Rapports Facebook** dans le menu.

Depuis un compte MyBitdefender :

1. Allez à : https://my.bitdefender.com.
2. Connectez-vous à votre compte à l'aide de votre nom d'utilisateur et de votre mot de passe.
3. Cliquez sur **Protection Facebook**.

   Un message vous informant que la protection Facebook n'est pas activée pour votre compte s'affiche.
4. Cliquez sur **Activer** pour poursuivre.

   Vous serez dirigé vers votre compte.
5. Utilisez vos informations de connexion Facebook pour vous connecter à l'application Safego.
6. Autoriser Safego à accéder à votre compte Facebook.

28. PROTECTION USB

La fonction AutoRun intégrée aux systèmes d'exploitation Windows est très utile car elle permet aux ordinateurs d'exécuter automatiquement un fichier depuis un support qui y est connecté. Par exemple, les installations de logiciels peuvent démarrer automatiquement lorsqu'un CD est inséré dans le lecteur optique.

Malheureusement, cette fonctionnalité peut également être utilisée par des malwares pour se lancer automatiquement et infiltrer votre ordinateur depuis des supports réinscriptibles tels que des lecteurs flash USB et des cartes mémoire connectés via des lecteurs de cartes. De nombreuses attaques exploitant la fonctionnalité AutoRun ont été créées ces dernières années.

Avec la protection USB, vous pouvez empêcher tout lecteur flash formaté en NTFS, FAT32 ou FAT d'exécuter des malwares. Lorsqu'un périphérique USB est immunisé, les malwares ne peuvent plus le configurer pour qu'il exécute une application spécifique lorsqu'il est connecté à un ordinateur fonctionnant sous Windows.

Pour immuniser un périphérique USB, procédez comme suit :

1. Connectez le lecteur flash à votre ordinateur.
2. Localisez sur votre ordinateur le périphérique de stockage amovible et faites un clic droit sur son icône.
3. Dans le menu contextuel, pointez sur **Bitdefender** et sélectionnez **Immuniser ce lecteur**.



Note
Si le lecteur a déjà été immunisé, le message **Le périphérique USB est protégé contre les malwares AutoRun** s'affichera au lieu de l'option Immuniser.

Pour empêcher que votre ordinateur ne lance des malwares depuis des lecteurs USB non immunisés, désactivez la fonction Exécution automatique des médias. Pour plus d'informations, consultez *« Utiliser la surveillance des vulnérabilités automatique »* (p. 136).

29. GÉRER VOS ORDINATEURS À DISTANCE

Votre compte MyBitdefender vous permet de gérer les produits Bitdefender installés sur vos ordinateurs à distance.

Utilisez MyBitdefender pour créer et appliquer à distance des tâches à vos ordinateurs.

Tout ordinateur sera géré depuis un compte MyBitdefender s'il remplit les conditions suivantes :

- vous avez installé un produit Bitdefender Internet Security 2015 sur l'ordinateur
- vous avez lié le produit Bitdefender au compte MyBitdefender.
- l'ordinateur est connecté à Internet

29.1. Accéder à MyBitdefender

Bitdefender vous permet de contrôler la sécurité de vos ordinateurs en ajoutant des tâches à vos produits Bitdefender.

Bitdefender vous permet d'accéder à votre compte MyBitdefender sur tout ordinateur ou appareil mobile connecté à Internet.

Accédez à MyBitdefender :

- Sur tout appareil avec un accès à Internet :
  1. Ouvrez un navigateur Web.
  2. Allez à :https://my.bitdefender.com
  3. Connectez-vous à votre compte à l'aide de votre nom d'utilisateur et de votre mot de passe.
- Depuis votre interface Bitdefender :
  1. Ouvrez la fenêtre de Bitdefender.
  2. Cliquez sur l'icône en haut de la fenêtre et sélectionnez **MyBitdefender** dans le menu déroulant.

29.2. Exécuter des tâches sur les ordinateurs

Pour exécuter une tâche sur l'un de vos ordinateurs, accédez à votre compte MyBitdefender.

En cliquant sur l'icône d'un ordinateur en bas de la fenêtre, vous pouvez voir toutes les tâches administratives que vous pouvez lancer sur cet ordinateur distant.

Enregistrement du produit
: Vous permet d'activer Bitdefender sur l'ordinateur distant en entrant une clé de licence.

Effectuer une analyse complète de votre PC
: Vous permet de lancer une analyse complète sur l'ordinateur distant.

Analyser les zones critiques pour détecter les malwares actifs
: Vous permet de lancer une analyse rapide sur l'ordinateur distant.

Corriger les problèmes critiques
: Vous permet de corriger les problèmes affectant la sécurité de l'ordinateur distant.

Mise à jour du produit
: Lance le processus de mise à jour du produit Bitdefender installé sur cet ordinateur.

OPTIMISATION DU SYSTÈME

30. OPTIMISATION

Bitdefender comporte un module Optimisation qui vous permet de préserver l'intégrité de votre système. Les outils de maintenance proposés sont essentiels pour améliorer la réactivité de votre système et pour gérer efficacement l'espace sur le disque dur.

Bitdefender vous propose les outils d'optimisation de PC suivants :

L'Optimisation en 1 clic analyse et améliore la vitesse de votre système en exécutant plusieurs tâches d'un simple clic sur un bouton.

L'Optimisation du démarrage réduit le temps de démarrage de votre système en empêchant l'exécution d'applications inutiles lorsque le PC est redémarré.

Nettoyage du PC - supprime les fichiers Internet temporaires et les cookies, les fichiers système inutilisés et les raccourcis vers les documents récents.

Défragmentation - réorganise physiquement les données sur le disque dur, de sorte que les différentes portions d'un fichier soient stockées les unes à la suite des autres, de façon continue.

Nettoyage du Registre - identifie et supprime les références non valides ou ayant expiré dans le Registre Windows. Pour conserver une base de registre de Windows propre et parfaitement optimisée, nous vous recommandons d'exécuter l'outil de nettoyage des registres tous les mois.

Restauration Registre - peut restaurer des clés de registre précédemment supprimées de la base de registre de Windows, en utilisant l'outil de nettoyage des registres de Bitdefender.

Détecteur de doublons - recherche et supprime les fichiers en double sur votre système.

30.1. Optimisation de la vitesse de votre système d'un simple clic

Des problèmes tels que des défaillances de disque dur, des fichiers de registre et un historique de navigateur restants peuvent ralentir le fonctionnement de votre ordinateur, ce qui peut devenir agaçant. Tout cela peut désormais être corrigé d'un simple clic sur un bouton.

L'Optimisation en 1 clic permet d'identifier et de supprimer les fichiers inutiles en exécutant plusieurs tâches de nettoyage à la fois.

Pour lancer le processus d'Optimisation en 1 clic, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Outils**.
3. Sous le module **Optimisation**, sélectionnez **Optimisation en 1 clic**. Pour quitter, cliquez sur **Annuler**.

    a. **Analyse**

    Patientez jusqu'à ce que Bitdefender ait terminé la recherche de problèmes associés au système.

    Nettoyage du Disque - identifie les anciens fichiers système inutiles.

    Nettoyage du Registre - identifie les références non valides ou ayant expiré dans le Registre Windows.

    Le Nettoyage des Données - identifie les fichiers Internet temporaires et les cookies, le cache et l'historique du navigateur.

    Le nombre de problèmes détectés s'affiche. Nous vous recommandons de les examiner avant de procéder au nettoyage. Cliquez sur **Optimisation** pour poursuivre.

    b. **Optimisation du système**

    Attendez que Bitdefender termine d'optimiser votre système.

    c. **Problèmes**

    Cette étape vous permet d'afficher le résultat de l'opération.

    Pour des informations complètes sur le processus d'optimisation, cliquez sur le lien **Afficher le rapport détaillé**.

30.2. Optimisation du temps de démarrage de votre PC

Un long démarrage du système est un véritable problème dû à des applications configurées pour s'exécuter alors qu'elles ne sont pas nécessaires. Attendre le démarrage du système pendant plusieurs minutes vous fait perdre un temps précieux et a un impact sur la productivité.

La fenêtre de l'Optimisation du démarrage affiche les applications en cours d'exécution au démarrage du système et vous permet de gérer leur comportement à cette étape.

Pour lancer le processus d'Optimisation du démarrage, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Outils**.
3. Sous le module **Optimisation**, sélectionnez **Optimisation du démarrage**.
   a. **Sélectionnez les applications**

      Vous pouvez voir une liste des applications qui s'exécutent au démarrage du système. Sélectionnez celles que vous souhaitez désactiver ou différer au démarrage.

   b. **Choix de la communauté**

      Découvrez ce que les autres utilisateurs de Bitdefender ont décidé de faire avec l'application que vous avez sélectionnée. En fonction de l'utilisation du programme, trois niveaux s'affichent : **Élevé**, **Moyen** et **Faible**.

   c. **Temps de démarrage du système**

      Le curseur en haut de la fenêtre indique le temps nécessaire à la fois à votre système et aux applications sélectionnées pour s'exécuter au démarrage.

      Un redémarrage du système est nécessaire pour obtenir des informations sur le temps de démarrage du système et des applications.

   d. **État du démarrage**

      Permettre. Sélectionnez cette option lorsque vous souhaitez qu'une application commence à s'exécuter au démarrage du système. Cette option est activée par défaut.

      Différer.

      Sélectionnez cette option pour reporter l'exécution d'un programme au démarrage du système.Cela signifie que les applications sélectionnées démarreront cinq minutes après la connexion de l'utilisateur au système.

La fonctionnalité **Différer** est prédéfinie et ne peut pas être configurée par l'utilisateur.

Désactiver. Sélectionnez cette option pour désactiver l'exécution d'un programme au démarrage du système.

e. **Résultats**

Des informations telles que l'estimation du temps de démarrage du système après le report ou la désactivation de l'exécution de programmes s'affichent.

Un redémarrage du système peut être requis pour voir toutes ces informations.

Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.



Note

Si votre abonnement expire ou si vous décidez de désinstaller Bitdefender, les paramètres par défaut des programmes dont vous avez décidé de bloquer l'exécution au démarrage seront restaurés.

30.3. Nettoyage de votre PC

Chaque fois que vous vous rendez sur une page Web, un fichier Internet temporaire est créé pour vous permettre d'accéder plus rapidement à cette page la prochaine fois.

Lorsque vous vous rendez sur une page Web, des cookies sont également stockés sur votre ordinateur.

L'assistant de nettoyage du PC vous aide à libérer de l'espace disque et à protéger votre vie privée en supprimant les fichiers qui ne sont plus utiles.

le cache des navigateurs (Internet Explorer, Mozilla Firefox, Google Chrome).

des informations de débogage (fichiers de rapport d'erreurs, fichiers dump et journaux créés par Windows lors de son fonctionnement).

des fichiers Windows inutiles (les fichiers de la corbeille et les fichiers système temporaires).

Pour lancer l'assistant de Nettoyage du PC, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Outils**.

3. Sous le panneau **Optimisation**, sélectionnez **Nettoyage du PC**.
4. Suivez cette procédure en trois étapes pour effectuer le nettoyage. Vous pouvez naviguer dans l'assistant à l'aide du bouton **Suivant**. Pour quitter l'assistant, cliquez sur **Annuler**.
   a. **Bienvenue dans le gestionnaire d'analyse**

      Sélectionnez **Standard** ou **Personnalisé**. Cliquez ensuite sur **Suivant** pour continuer.

   b. **Lancer un nettoyage**
   c. **Résultats**

30.4. Défragmenter des volumes de disque dur

La fragmentation de fichiers intervient lors de la copie d'un fichier excédant le plus grand bloc d'espace libre du disque dur. Étant donné que l'espace libre est insuffisant pour y stocker l'intégralité du fichier en continu, celui-ci est stocké en plusieurs blocs. Les données du fichier fragmenté doivent être lues à partir de plusieurs emplacements différents.

Il est recommandé de défragmenter le disque dur pour:

accéder aux fichiers plus rapidement ;
améliorer la performance globale du système ;
augmenter la durée de vie du disque dur.

Pour lancer l'assistant du défragmenteur de disque, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Outils**.
3. Sous le panneau **Optimisation**, sélectionnez **Défragmentation**.
4. Suivez cette procédure en cinq étapes pour effectuer la défragmentation. Vous pouvez naviguer dans l'assistant à l'aide du bouton **Suivant**. Pour quitter l'assistant, cliquez sur **Annuler**.
   a. **Sélectionner pour l'analyse**

      Sélectionnez les partitions dont vous souhaitez vérifier la fragmentation. Cliquez sur **Continuer** pour lancer le processus d'analyse.

   b. **Analyse**

      Patientez jusqu'à ce que Bitdefender ait terminé l'analyse des partitions.

c. **Sélectionner pour la défragmentation**

L'état de la fragmentation des partitions analysées est affiché. Sélectionnez les partitions que vous souhaitez défragmenter.

d. **Défrag.**

Veuillez attendre que Bitdefender ait fini de défragmenter les partitions.

e. **Résultats**



Note

La défragmentation peut prendre un certain temps sachant qu'elle implique de déplacer des parties de données stockées d'un emplacement du disque dur à un autre. Nous vous recommandons d'effectuer la défragmentation lorsque vous n'utilisez pas votre ordinateur.

30.5. Nettoyer le registre Windows

De nombreuses applications enregistrent des clés dans cette base au moment de leur installation. Lorsque ces applications sont supprimées, certaines de leurs clés associées peuvent ne pas être supprimées et demeurer dans la base de registre, ce qui ralentit le système et peut même provoquer son instabilité. Il en va de même lorsque vous supprimez des raccourcis vers certains fichiers d'applications installés dans votre système ou dans le cas de pilotes corrompus.

Pour lancer l'assistant de nettoyage du registre, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Outils**.
3. Sous le panneau **Optimisation**, sélectionnez **Nettoyage du Registre**.
4. Suivez la procédure en quatre étapes pour nettoyer le registre. Vous pouvez naviguer dans l'assistant à l'aide du bouton **Suivant**. Pour quitter l'assistant, cliquez sur **Annuler**.

   a. **Bienvenue dans le gestionnaire d'analyse**

   b. **Effectuer l'analyse**

   Patientez jusqu'à ce que Bitdefender ait terminé l'analyse du registre.

   c. **Sélectionner les clés**

Vous pouvez voir toutes les clés de registre non valides ou orphelines détectées. Chacune est accompagnée d'informations détaillées la concernant (nom, valeur, priorité, catégorie).

Les clés de registre sont regroupées selon leur emplacement dans le registre Windows :

Répertoires de logiciels. Clés de registre contenant des informations sur les chemins des applications installées sur votre ordinateur.

Les clés non valides sont indexées en priorité basse, ce qui signifie que vous pouvez les effacer en ne prenant quasiment aucun risque.

Commandes personnalisées. Clés de registre contenant des informations sur les extensions de fichiers enregistrées sur votre ordinateur.Ces clés de registre sont généralement utilisées pour conserver les associations de fichiers (pour s'assurer que le bon programme s'ouvre quand vous ouvrez un fichier en utilisant Windows Explorer).Par exemple, une telle clé de registre autorise Windows à ouvrir un fichier .doc dans Microsoft Word.

Les clés non valides sont indexées en priorité basse, ce qui signifie que vous pouvez les effacer en ne prenant quasiment aucun risque.

Les DLL partagées. Clés de registre contenant des informations sur l'emplacement des DLLs partagés (Dynamic Link Libraries).Les fichiers DLL intègrent des fonctions qui sont utilisées par les applications installées pour effectuer certaine tâches. Elles peuvent être partagées par de multiples applications pour réduire la prise de ressource en mémoire ou en espace disque.

Ces clés de registres deviennent non valides quand les DLL vers lesquelles elles pointent sont déplacées dans un emplacement différent ou sont supprimées (c'est ce qui se produit généralement quand vous désinstallez un programme.)

Les clés non valides sont indexées avec une priorité moyenne, ce qui veut dire que les effacer peut avoir des conséquences négatives sur le système.

Par défaut, toutes les clés sont sélectionnées pour être supprimées. Vous pouvez choisir de supprimer individuellement des clés non valides d'une catégorie sélectionnée.

d. **Résultats**

30.6. Restauration du registre nettoyé

Il est possible qu'après un nettoyage des registres, votre système ne fonctionne pas correctement ou que certaines applications présentent des dysfonctionnements dus à des clés de registre manquantes. Cela peut provenir de clés de registre partagées ayant été supprimées lors du nettoyage des registres ou d'autres clés supprimées. Pour résoudre ce problème, vous devez restaurer les registres nettoyés.

Pour lancer l'assistant de récupération du registre, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Outils**.
3. Sous le panneau **Optimisation**, sélectionnez **Restauration du Registre**.
4. Suivez cette procédure en deux étapes pour récupérer le registre nettoyé. Vous pouvez naviguer dans l'assistant à l'aide du bouton **Suivant**. Pour quitter l'assistant, cliquez sur **Annuler**.
   a. **Point de contrôle**

      Vous pouvez voir une liste de moments spécifiques auxquels la base de registre de Windows a été nettoyée. Cliquez sur le lien **Afficher le Fichier** pour voir les clés de registre détectées. Sélectionnez un moment spécifique pour appliquer la restauration de la base de registre de Windows.

      Avertissement
      Il se peut que la restauration des registres nettoyés écrase les clés de registre modifiées depuis le dernier nettoyage des registres.

   b. **Résultats de la tâche**

30.7. Rechercher les doublons

Les doublons consomment beaucoup d'espace sur le disque dur. Imaginez le même fichier .mp3 stocké à trois emplacements différents.

L'assistant du détecteur de doublons vous aidera à détecter et à supprimer les fichiers en double sur votre ordinateur.

Pour lancer le détecteur de doublons, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.

2. Accédez au panneau **Outils**.
3. Sous le panneau **Optimisation**, sélectionnez **Détecteur de doublons**.
4. Suivez la procédure en quatre étapes pour identifier et supprimer les doublons. Vous pouvez naviguer dans l'assistant à l'aide du bouton **Suivant**. Pour quitter l'assistant, cliquez sur **Annuler**.

   a. **Sélectionner la cible**

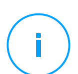
      Ajoutez les dossiers où vous souhaitez rechercher les fichiers en double.

   b. **Rechercher les doublons**

      Patientez jusqu'à ce que Bitdefender ait terminé la recherche de doublons.

   c. **Fichiers à supprimer**

      Les fichiers identiques figurent dans des groupes. Vous pouvez choisir une action à mener sur tous les groupes ou séparément sur chaque groupe : conserver le plus récent, conserver le plus ancien ou ne rien faire. Vous pouvez aussi sélectionner des actions pour chaque fichier individuel.

      Note
      Si aucun doublon n'est détecté, cette étape sera ignorée.

   d. **Résultats**

31. PROFILS

Effectuer des activités professionnelles quotidiennes, regarder des films ou jouer peut ralentir le système, en particulier si des processus de mise à jour Windows et des tâches de maintenance ont lieu simultanément. Bitdefender vous permet désormais de choisir et d'appliquer le profil de votre choix, qui fait les réglages nécessaires pour améliorer les performances de certaines applications installées sur le système.

Bitdefender propose les profils suivants :

- Profil Travail
- Profil Film
- Profil Jeu

Si vous décidez de ne pas utiliser les **Profils**, un profil par défaut nommé **Standard** est activé et n'apporte aucune optimisation à votre système.

En fonction de votre activité, les paramètres du produit suivants s'appliquent lorsqu'un profil est activé :

- Toutes les alertes et fenêtres pop-up de Bitdefender sont désactivées.
- La Mise à jour Automatique est reportée.
- Les analyses planifiées sont reportées.
- Search Advisor est désactivé.
- La Détection d'Intrusion est réglée sur le niveau de protection **Tolérant**.
- Les offres spéciales et notifications du produit sont désactivées.

En fonction de votre activité, les paramètres du système suivants s'appliquent lorsqu'un profil est activé :

- Les mises à jour automatiques de Windows sont reportées.
- Les alertes et fenêtres pop-up de Windows sont désactivées.
- Les programmes inutiles en arrière-plan sont interrompus.
- Les effets visuels sont ajustés pour de meilleures performances.
- Les tâches de maintenance sont reportées.
- Les paramètres du plan d'alimentation sont adaptés.

31.1. Profil Travail

Effectuer plusieurs tâches au travail comme envoyer des e-mails, avoir une communication vidéo avec des collègues ou utiliser des applications de conception graphique peut affecter les performances de votre système. Le profil Travail est conçu pour vous aider à améliorer votre efficacité en désactivant certaines tâches de maintenance et services d'arrière-plan.

Configurer le Profil Travail

Pour configurer les actions à appliquer lorsque le Profil Travail est activé, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Outils**.
3. Cliquez sur le module **Profils**.
4. Dans la fenêtre **Paramètres des profils**, cliquez sur le bouton **Configurer** dans la zone Profil Travail.
5. Sélectionnez les réglages du système que vous souhaitez appliquer en cochant les options suivantes :

   Améliorer les performances pour les applications de bureautique

   Optimiser les paramètres du produit pour le profil Travail

   Reporter les tâches de maintenance et les programmes en arrière-plan

   Reporter les mises à jour automatiques de Windows
6. Cliquez sur **Enregistrer** pour sauvegarder les modifications et fermer la fenêtre.

Ajouter manuellement des applications à la liste du Profil Travail

Si Bitdefender ne passe pas automatiquement en Profil Travail lorsque vous lancez une application de travail spécifique, vous pouvez ajouter manuellement cette application à la **Liste des applications**.

Pour ajouter manuellement des applications à la Liste des applications dans le Profil Travail :

1. Ouvrez la fenêtre de Bitdefender.

2. Accédez au panneau **Outils**.
3. Cliquez sur le module **Profils**.
4. Dans la fenêtre **Profils**, cliquez sur le bouton **Configurer** dans la zone Profil Travail.
5. Dans la fenêtre **Profil Travail**, cliquez sur le lien **Liste des applications**.
6. Cliquez sur **Ajouter** pour ajouter une nouvelle application à la **Liste des applications**.

   Une nouvelle fenêtre s'affiche. Localisez le fichier exécutable de l'application, sélectionnez-le et cliquez sur **OK** pour l'ajouter à la liste.

31.2. Profil Film

Afficher du contenu vidéo de grande qualité comme des films haute définition nécessite d'importantes ressources système.Le Profil Film ajuste la configuration du système et du logiciel afin que vous puissiez regarder des films sans interruptions.

Configurer le Profil Film

Pour configurer les actions à appliquer lorsque le profil Film est activé :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Outils**.
3. Cliquez sur le module **Profils**.
4. Dans la fenêtre **Paramètres des profils**, cliquez sur le bouton **Configurer** dans la zone Profil Film.
5. Sélectionnez les réglages du système que vous souhaitez appliquer en cochant les options suivantes :

   Améliorer les performances pour les lecteurs vidéo

   Optimiser les paramètres du produit pour le profil Film

   Reporter les tâches de maintenance et les programmes en arrière-plan

   Reporter les mises à jour automatiques de Windows

   Ajuster les paramètres du plan d'alimentation pour les films
6. Cliquez sur **Enregistrer** pour sauvegarder les modifications et fermer la fenêtre.

Ajouter manuellement des lecteurs vidéo à la liste du Profil Film

Si Bitdefender ne passe pas automatiquement en Profil Film lorsque vous lancez un lecteur vidéo spécifique, vous pouvez ajouter manuellement cette application à la **Liste des lecteurs vidéo**.

Pour ajouter manuellement des lecteurs vidéo à la Liste des lecteurs vidéo dans le Profil Film :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Outils**.
3. Cliquez sur le module **Profils**.
4. Dans la fenêtre **Paramètres des profils**, cliquez sur le bouton **Configurer** dans la zone Profil Film.
5. Dans la fenêtre **Profil Film**, cliquez sur le lien **Liste des lecteurs vidéo**.
6. Cliquez sur **Ajouter** pour ajouter une nouvelle application à la **Liste des lecteurs vidéo**.

   Une nouvelle fenêtre s'affiche. Localisez le fichier exécutable de l'application, sélectionnez-le et cliquez sur **OK** pour l'ajouter à la liste.

31.3. Profil Jeu

Pour une meilleure expérience de jeu, il suffit de réduire les interruptions du système et de diminuer les ralentissements.En associant des techniques heuristiques comportementales à une liste de jeux connus, Bitdefender détecte automatiquement les jeux en cours d'exécution et optimise les ressources du système afin que vous puissiez profiter pleinement de vos pauses.

Configurer le Profil Jeu

Pour configurer les actions à appliquer lorsque le Profil Jeu est activé, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Outils**.
3. Cliquez sur le module **Profils**.

4. Dans la fenêtre **Paramètres des profils**, cliquez sur le bouton **Configurer** dans la zone Profil Jeu.
5. Sélectionnez les réglages du système que vous souhaitez appliquer en cochant les options suivantes :

   Améliorer les performances pour les jeux

   Optimiser les paramètres du produit pour le profil Jeu

   Reporter les tâches de maintenance et les programmes en arrière-plan

   Reporter les mises à jour automatiques de Windows

   Ajuster les paramètres du plan d'alimentation pour les jeux
6. Cliquez sur **Enregistrer** pour sauvegarder les modifications et fermer la fenêtre.

Ajouter manuellement des jeux à la Liste des jeux.

Si Bitdefender ne passe pas automatiquement en Profil Jeu lorsque vous lancez un jeu ou une application spécifique, vous pouvez ajouter manuellement cette application à la **Liste des Jeux**.

Pour ajouter manuellement des jeux à la liste des Jeux dans le Profil Jeu :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Outils**.
3. Cliquez sur le module **Profils**.
4. Dans la fenêtre **Paramètres des profils**, cliquez sur le bouton **Configurer** dans la zone Profil Jeu.
5. Dans la fenêtre **Profil Jeu**, cliquez sur le lien **Liste des Jeux**.
6. Cliquez sur **Ajouter** pour ajouter un nouveau jeu à la **Liste des Jeux**.

   Une nouvelle fenêtre s'affiche. Localisez le fichier exécutable du jeu, sélectionnez-le et cliquez sur **OK** pour l'ajouter à la liste.

31.4. Optimisation en temps réel

L'Optimisation en temps réel de Bitdefender est un plugin qui améliore les performances de votre système discrètement, en arrière-plan, en veillant à ce que vous ne soyez pas interrompu lorsque vous êtes en mode profil. En fonction de la charge du processeur, le plugin surveille tous les processus,

en particulier ceux qui ont une charge plus élevée, afin de les adapter à vos besoins.

Pour activer ou désactiver l'Optimisation en temps réel, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Outils**.
3. Cliquez sur le module **Profils**.
4. Dans la fenêtre **Profils**, sélectionnez l'onglet **Paramètres des profils.**
5. Activez ou désactivez l'Optimisation en temps réel en cliquant sur le bouton correspondant.

RÉSOLUTION DES PROBLÈMES

32. RÉSOUDRE LES PROBLÈMES LES PLUS FRÉQUENTS

Ce chapitre présente certains problèmes que vous pouvez rencontrer lorsque vous utilisez Bitdefender et vous fournit des solutions possibles à ces problèmes.La plupart de ces problèmes peuvent être résolus via la configuration appropriée des paramètres du produit.

« *Mon système semble lent* » (p. 196)

« *L'analyse ne démarre pas* » (p. 198)

« *Je ne peux plus utiliser une application* » (p. 201)

« *Que faire lorsque Bitdefender bloque un site web ou une application en ligne sûre* » (p. 202)

« *Comment mettre à jour Bitdefender avec une connexion Internet lente* » (p. 207)

« *Mon ordinateur n'est pas connecté à Internet. Comment actualiser Bitdefender?* » (p. 207)

« *Le Services Bitdefender ne répondent pas* » (p. 208)

« *Le filtre antispam ne fonctionne pas correctement* » (p. 209)

« *La fonctionnalité saisie automatique de mon Portefeuille ne fonctionne pas* » (p. 214)

« *La désinstallation de Bitdefender a échoué* » (p. 215)

« *Mon système ne démarre pas après l'installation de Bitdefender* » (p. 217)

Si vous ne parvenez pas à trouver votre problème ici, ou si les solutions présentées ne le résolvent pas, vous pouvez contacter les représentants du soutien technique Bitdefender comme indiqué dans le chapitre « *Demander de l'aide* » (p. 233).

32.1. Mon système semble lent

Généralement, après l'installation d'un logiciel de sécurité, on assiste à un léger ralentissement du système, qui est normal dans une certaine mesure.

Si vous remarquez un ralentissement important, ce problème peut apparaître pour les raisons suivantes :

Bitdefender n'est pas le seul logiciel de sécurité installé sur le système.

Bien que Bitdefender recherche et supprime les programmes de sécurité trouvés pendant l'installation, il est recommandé de supprimer tout programme antivirus que vous utilisiez avant d'installer Bitdefender.Pour plus d'informations, consultez *« Comment supprimer les autres solutions de sécurité ? »* (p. 86).

Vous ne disposez pas de la configuration système minimale pour l'exécution de Bitdefender.

Si votre machine ne dispose pas de la configuration système minimale, l'ordinateur deviendra lent, notamment lorsque plusieurs applications s'exécuteront simultanément. Pour plus d'informations, consultez *« Configuration système minimale »* (p. 3).

Il reste trop de clés de registre non valides dans votre registre Windows.

Le nettoyage du registre Windows peut améliorer les performances de votre système. Pour plus d'informations, consultez *« Nettoyer le registre Windows »* (p. 185).

Vos disques durs sont trop fragmentés.

La fragmentation de fichiers ralentit l'accès aux fichiers et fait diminuer les performances système.

L'exécution du défragmenteur de disque peut améliorer les performances de votre système.Pour plus d'informations, consultez *« Défragmenter des volumes de disque dur »* (p. 184).

Pour défragmenter votre disque en utilisant votre système d'exploitation Windows, suivez ce chemin à partir du menu démarrer de Windows : **Démarrer** → **Tous les programmes** → **Accessoires** → **Outils système** → **Défragmenteur de disque**.

Vous avez installé des applications que vous n'utilisez pas.

Tous les ordinateurs ont des programmes ou des applications qui ne sont pas utilisés. Et de nombreux programmes indésirables s'exécutent en tâche de fond, utilisant de l'espace disque et de la mémoire. Si vous n'utilisez pas un programme, désinstallez-le. Cela s'applique également à tout autre logiciel préinstallé ou version d'évaluation d'une application que vous avez oublié de désinstaller.



Important

Si vous pensez qu'un programme ou qu'une application pourrait constituer un élément essentiel de votre système d'exploitation, ne les désinstallez pas et contactez le Service Client de Bitdefender pour obtenir de l'aide.

Votre système peut être infecté.

La vitesse de votre système et son comportement général peuvent également être affectés par des malwares. Les logiciels espions, les virus, les chevaux de Troie et les publiciels nuisent tous aux performances de votre ordinateur. Veillez à analyser votre système régulièrement, au moins une fois par semaine. Il est recommandé d'utiliser l'Analyse du système Bitdefender car elle recherche tous les types de malwares menaçant la sécurité de votre système.

Pour lancer l'analyse du système, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Sous le module **Antivirus**, sélectionnez **Analyse du Système**.
4. Suivez les étapes de l'assistant.

32.2. L'analyse ne démarre pas

Ce type de problème peut avoir deux causes principales :

Une installation précédente de Bitdefender qui n'a pas été complètement supprimée ou une installation défectueuse de Bitdefender.

Dans ce cas, procédez comme suit :

1. Désinstaller complètement Bitdefender du système :

   Dans **Windows XP**:

   a. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Ajout/Suppression de programmes**.

   b. Localisez **Bitdefender Internet Security 2015** et sélectionnez **Supprimer**.

   c. Cliquez sur **Supprimer** dans la fenêtre qui apparaît puis sélectionnez **Je souhaite le réinstaller**.

d. Attendez la fin du processus de désinstallation et puis redémarrez votre système.

Dans **Windows Vista** et **Windows 7**:

a. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.

b. Localisez **Bitdefender Internet Security 2015** et sélectionnez **Désinstaller**.

c. Cliquez sur **Supprimer** dans la fenêtre qui apparaît puis sélectionnez **Je souhaite le réinstaller**.

d. Attendez la fin du processus de désinstallation et puis redémarrez votre système.

Dans **Windows 8** :

a. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.

b. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.

c. Localisez **Bitdefender Internet Security 2015** et sélectionnez **Désinstaller**.

d. Cliquez sur **Supprimer** dans la fenêtre qui apparaît puis sélectionnez **Je souhaite le réinstaller**.

e. Attendez la fin du processus de désinstallation et puis redémarrez votre système.

2. Réinstallez votre produit Bitdefender.

Bitdefender n'est pas la seule solution de sécurité installée sur votre système.

Dans ce cas, procédez comme suit :

1. Supprimer l'autre solution de sécurité. Pour plus d'informations, consultez *« Comment supprimer les autres solutions de sécurité ? »* (p. 86).
2. Désinstaller complètement Bitdefender du système :

Dans **Windows XP**:

a. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Ajout/Suppression de programmes**.
b. Localisez **Bitdefender Internet Security 2015** et sélectionnez **Supprimer**.
c. Cliquez sur **Supprimer** dans la fenêtre qui apparaît puis sélectionnez **Je souhaite le réinstaller**.
d. Attendez la fin du processus de désinstallation et puis redémarrez votre système.

Dans **Windows Vista** et **Windows 7**:

a. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
b. Localisez **Bitdefender Internet Security 2015** et sélectionnez **Désinstaller**.
c. Cliquez sur **Supprimer** dans la fenêtre qui apparaît puis sélectionnez **Je souhaite le réinstaller**.
d. Attendez la fin du processus de désinstallation et puis redémarrez votre système.

Dans **Windows 8** :

a. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
b. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.
c. Localisez **Bitdefender Internet Security 2015** et sélectionnez **Désinstaller**.
d. Cliquez sur **Supprimer** dans la fenêtre qui apparaît puis sélectionnez **Je souhaite le réinstaller**.
e. Attendez la fin du processus de désinstallation et puis redémarrez votre système.

3. Réinstallez votre produit Bitdefender.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Demander de l'aide* » (p. 233).

32.3. Je ne peux plus utiliser une application

Ce problème se produit lorsque vous essayez d'utiliser un programme qui fonctionnait normalement avant d'installer Bitdefender.

Après l'installation de Bitdefender vous pouvez vous trouver dans l'une des situations suivantes :

Vous pourriez recevoir un message de Bitdefender indiquant que le programme essaie d'apporter une modification au système.

Il est possible que vous receviez un message d'erreur du programme que vous tentez d'utiliser.

Ce type de situation se produit quand Active Virus Control détecte à tort certaines applications comme étant malveillantes.

Active Virus Control est un module Bitdefender qui surveille en permanence les applications s'exécutant sur votre système et signale celles au comportement potentiellement malveillant. Étant donné que la fonction est basée sur un système heuristique, des applications légitimes peuvent, dans certains cas, être signalées par le contrôle actif de virus.

Lorsque cette situation se produit, vous pouvez empêcher l'application correspondante d'être surveillée par le contrôle actif de virus.

Pour ajouter le programme à la liste d'exceptions, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Antivirus**.
4. Dans la fenêtre **Antivirus**, sélectionnez l'onglet **Exclusions**.
5. Cliquez sur le lien **Processus Exclus**. Dans la fenêtre qui apparaît, vous pouvez gérer les exclusions de processus du contrôle actif de virus.
6. Ajoutez des exclusions en suivant ces étapes :
   a. Cliquez sur le bouton **Ajouter**, situé en haut du tableau des exclusions.
   b. Cliquez sur **Parcourir**, sélectionnez l'application que vous souhaitez exclure, puis cliquez sur **OK**.
   c. Gardez l'option **Autoriser** sélectionnée pour empêcher le contrôle actif de virus de bloquer l'application.
   d. Cliquez sur **Ajouter**.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section *« Demander de l'aide »* (p. 233).

32.4. Que faire lorsque Bitdefender bloque un site web ou une application en ligne sûre

Bitdefender permet de naviguer sur Internet en toute sécurité en filtrant l'ensemble du trafic web et en bloquant tout contenu malveillant. Il est toutefois possible que Bitdefender considère à tort qu'un site web ou une application en ligne n'est pas sûr, et que l'analyse du trafic HTTP de Bitdefender les bloque par erreur.

Si une page ou une application est bloquée de façon répétée, elle peut être ajoutée à une liste blanche afin de ne pas être analysée par les moteurs de Bitdefender et de permettre une navigation sans interruptions.

Pour ajouter un site web à la **Liste blanche**, procédez comme suit :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Protection Web**.
4. Dans l'onglet **Configuration**, cliquez sur le lien **Liste blanche**. Une nouvelle fenêtre s'affiche.
5. Indiquez l'adresse du site web ou d'une application en ligne bloquée dans le champ correspondant et cliquez sur **Ajouter**.
6. Cliquez sur **Enregistrer** pour sauvegarder les modifications et fermer la fenêtre.

Seuls les sites web et les applications en lesquels vous avez pleinement confiance devraient être ajoutés à cette liste. Ils ne seront pas analysés par les moteurs suivants : malwares, phishing et fraude.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section *« Demander de l'aide »* (p. 233).

32.5. Je ne peux pas me connecter à Internet

Vous remarquerez peut-être qu'un programme ou un navigateur web ne peut plus se connecter à Internet ou accéder aux services réseau après avoir installé Bitdefender.

Dans ce cas, la meilleure solution est de configurer Bitdefender afin qu'il autorise automatiquement les connexions de et vers l'application logicielle en question :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Pare-feu**.
4. Dans la fenêtre **Pare-feu**, sélectionnez l'onglet **Règles**.
5. Pour ajouter une règle d'application, cliquez sur le bouton **Ajouter une règle**.
6. Une nouvelle fenêtre apparaît dans laquelle vous pouvez ajouter les informations. Veillez à sélectionner tous les types de réseau disponibles et sélectionnez **Autoriser** dans la section **Permission**.

Fermez Bitdefender, ouvrez l'application logicielle et réessayez de vous connecter à Internet.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Demander de l'aide* » (p. 233).

32.6. Je ne peux pas accéder à un périphérique de mon réseau

En fonction du réseau auquel vous êtes connecté, le pare-feu Bitdefender peut bloquer la connexion entre votre système et un autre périphérique (tel qu'un ordinateur ou une imprimante). Vous ne pouvez donc plus partager ou imprimer des fichiers.

Dans ce cas, la meilleure solution est de configurer Bitdefender afin qu'il autorise automatiquement les connexions de et vers le périphérique en question. Pour chaque connexion réseau vous pouvez configurer une zone spéciale de confiance.

Une zone de confiance est un périphérique auquel vous faites entièrement confiance. Tout le trafic entre votre ordinateur et le périphérique de confiance est autorisé. Pour partager des ressources avec des périphériques spécifiques, tels que des ordinateurs ou des imprimantes, ajoutez-les comme zones de confiance.

Pour ajouter une zone de confiance sur vos cartes réseau, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Pare-feu**.
4. Dans la fenêtre **Pare-feu**, sélectionnez l'onglet **Règles**.
5. Pour ajouter une zone, cliquez sur le bouton **Ajouter une règle**. Une nouvelle fenêtre affichant les adresses IP des périphériques connectés au réseau s'affichera.
6. Sélectionnez l'adresse IP de l'ordinateur ou de l'imprimante que vous souhaitez ajouter, ou tapez une adresse ou une plage d'adresses dans la zone de texte prévue à cet effet.
7. Dans le champ **Permission** sélectionnez **Autoriser** puis cliquez sur **OK**.

Si vous ne pouvez toujours pas vous connecter au périphérique, le problème n'est peut-être pas causé par Bitdefender.

Vérifiez d'autres causes possibles, telles que les suivantes :

Le pare-feu de l'autre ordinateur peut bloquer le partage de fichiers et d'imprimantes avec celui-ci.

Si le pare-feu Windows est utilisé, il peut être configuré pour autoriser le partage de fichiers et d'imprimantes comme suit :

– Dans **Windows XP**:
  1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et sélectionnez **Centre de sécurité**.
  2. Ouvrez les paramètres du pare-feu Windows et sélectionnez l'onglet **Exceptions**.
  3. Cochez la case **Partage de fichiers et d'imprimantes**.
– Dans **Windows Vista et Windows 7** :
  1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et sélectionnez **Système et sécurité**.
  2. Allez dans **Pare-feu Windows** et cliquez sur **Autoriser un programme via le Pare-feu Windows**.
  3. Cochez la case **Partage de fichiers et d'imprimantes**.
– Dans **Windows 8** :

1. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
2. Cliquez sur **Système et sécurité**, allez dans **Pare-feu Windows** et sélectionnez **Autoriser une application via le pare-feu Windows**.
3. Cochez la case **Partage de fichiers et d'imprimantes** et cliquez sur **OK**.

Si un autre programme pare-feu est utilisé, veuillez vous reporter à sa documentation ou au fichier d'aide.

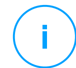
Conditions générales pouvant empêcher d'utiliser ou de se connecter à une imprimante partagée :

Il se peut que vous ayez besoin de vous connecter à un compte Windows administrateur pour avoir accès à l'imprimante partagée.

L'imprimante partagée est configurée pour autoriser l'accès uniquement à certains ordinateurs et utilisateurs. Si vous partagez votre imprimante, vérifiez que l'imprimante autorise l'accès à l'utilisateur de l'autre ordinateur. Si vous essayez de vous connecter à une imprimante partagée, vérifiez avec l'utilisateur de l'autre ordinateur que vous êtes autorisé(e) à vous connecter à l'imprimante.

L'imprimante connectée à votre ordinateur ou à l'autre ordinateur n'est pas partagée.

L'imprimante partagée n'a pas été ajoutée à l'ordinateur.



Note

Pour apprendre à gérer le partage d'imprimante (partager une imprimante, définir ou supprimer des permissions pour une imprimante, se connecter à l'imprimante d'un réseau ou à une imprimante partagée) consultez le Centre d'aide et de support de Windows (dans le menu Démarrer, cliquez sur **Aide et Support**).

L'accès à une imprimante réseau peut être limité à des ordinateurs et des utilisateurs spécifiques uniquement. Consultez l'administrateur réseau pour savoir si vous avez l'autorisation de vous connecter à cette imprimante.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section *« Demander de l'aide »* (p. 233).

32.7. Mon Internet est lent

Cette situation peut se produire après l'installation de Bitdefender. Le problème pourrait être causé par des erreurs dans la configuration du pare-feu de Bitdefender.

Pour régler cette situation, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Cliquez sur le module **Pare-feu**.
4. Dans la fenêtre **Pare-feu**, cliquez sur le bouton pour désactiver le **Pare-feu**.
5. Vérifiez si votre connexion Internet s'est améliorée avec le pare-feu Bitdefender désactivé.

   Si votre connexion à Internet est toujours lente, le problème n'est peut-être pas causé par Bitdefender. Nous vous recommandons de contacter votre fournisseur d'accès à Internet afin de vérifier si la connexion est opérationnelle de son côté.

   Si vous recevez la confirmation de votre fournisseur d'accès à Internet que la connexion est opérationnelle de leur côté et que le problème persiste, contactez Bitdefender comme cela est décrit dans la section *« Demander de l'aide »* (p. 233).

   Si la connexion Internet s'est améliorée après la désactivation du pare-feu Bitdefender, suivez ces étapes :

   a. Ouvrez la fenêtre de Bitdefender.
   b. Accédez au panneau **Protection**.
   c. Cliquez sur le module **Pare-feu**.
   d. Dans la fenêtre **Pare-feu**, sélectionnez l'onglet **Configuration**.
   e. Allez dans **Bloquer le partage de connexion Internet** et cliquez sur le bouton pour l'activer.
   f. Allez dans **Bloquer les analyses de port dans le réseau** et cliquez sur le bouton pour le désactiver.

g. Allez dans l'onglet **Adaptateurs** et sélectionnez votre connexion Internet.

h. Dans la colonne **Type de Réseau**, sélectionnez **Domicile/Bureau**.

i. Dans la colonne **Mode Furtif** sélectionnez **Distant**. Réglez la colonne **Générique** sur **Activé**.

j. Fermez Bitdefender, redémarrez le système et vérifiez la vitesse de la connexion à Internet.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Demander de l'aide* » (p. 233).

32.8. Comment mettre à jour Bitdefender avec une connexion Internet lente

Si votre connexion Internet est lente (RTC ou RNIS, par exemple), des erreurs peuvent se produire pendant le processus de mise à jour.

Pour maintenir votre système à jour avec les dernières signatures de malwares Bitdefender, suivez les étapes suivantes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur l'icône en haut de la fenêtre et sélectionnez **Paramètres généraux** dans le menu déroulant.
3. Dans la fenêtre **Paramètres généraux**, sélectionnez l'onglet **Mise à jour**.
4. À côté de **Règles de traitement**, sélectionnez **Demander avant le téléchargement** dans le menu déroulant.
5. Retournez dans la fenêtre principale et cliquez sur le bouton d'action **Mise à jour** à droite de la fenêtre.
6. Sélectionnez uniquement **Mises à jour de signatures**, puis cliquez sur **OK**.
7. Bitdefender ne téléchargera et n'installera que les mises à jour des signatures de malwares.

32.9. Mon ordinateur n'est pas connecté à Internet. Comment actualiser Bitdefender?

Si votre ordinateur n'est pas connecté à Internet, vous devez télécharger manuellement les mises à jour sur un ordinateur avec accès Internet, puis

les transférer sur votre ordinateur à l'aide d'un dispositif amovible comme une clé USB.

Suivez ces étapes :

1. Sur un ordinateur connecté à Internet, ouvrez le navigateur Web et allez sur :

   http://www.bitdefender.fr/site/view/Desktop-Products-Updates.html

2. Dans la colonne **Mise à jour Manuelle**, cliquez sur le lien correspondant à votre produit et à votre architecture système. Si vous ignorez si votre version de Windows est de 32 ou 64 bits, reportez-vous à « *Est-ce que j'utilise une version de Windows de 32 ou 64 bits ?* » (p. 85).
3. Enregistrez le fichier nommé weekly.exe dans le système.
4. Transférez le fichier téléchargé sur un support amovible comme une clé USB, puis sur votre ordinateur.
5. Double-cliquez sur le fichier, puis suivez les étapes de l'assistant.

32.10. Le Services Bitdefender ne répondent pas

Cet article vous aide à régler l'erreur **Les Services Bitdefender ne répondent pas**. Vous pouvez rencontrer cette erreur de la façon suivante :

L'icône Bitdefender de la zone de notification est grisée et vous informe que les services Bitdefender ne répondent pas.

La fenêtre Bitdefender indique que les services Bitdefender ne répondent pas.

L'erreur peut être causée par :

erreurs de communication temporaires entre les services Bitdefender.

certains services Bitdefender sont interrompus.

d'autres solutions de sécurité sont en cours d'exécution sur votre ordinateur en même temps que Bitdefender.

Pour régler cette erreur, essayez ces solutions :

1. Attendez quelques instants et voyez si quelque chose change. L'erreur peut être temporaire.

2. Redémarrez l'ordinateur et attendez quelques instants jusqu'à ce que Bitdefender soit chargé. Ouvrez Bitdefender pour voir si l'erreur persiste. Redémarrer l'ordinateur règle habituellement le problème.
3. Vérifiez que vous n'avez pas d'autre solution de sécurité installée car cela pourrait affecter le fonctionnement normal de Bitdefender. Si c'est le cas, nous vous recommandons de supprimer toutes les autres solutions de sécurité et de réinstaller ensuite Bitdefender.

   Pour plus d'informations, consultez *« Comment supprimer les autres solutions de sécurité ? »* (p. 86).

Si l'erreur persiste, veuillez contacter les représentants de notre soutien technique pour obtenir de l'aide, comme indiqué dans la section *« Demander de l'aide »* (p. 233).

32.11. Le filtre antispam ne fonctionne pas correctement

Cet article aide à régler les problèmes suivants avec le filtrage Antispam Bitdefender :

Certains e-mails légitimes sont signalés comme étant du [spam].

De nombreux messages de spam ne sont pas signalés comme tels par le filtre antispam.

Le filtre antispam ne détecte aucun message de spam.

32.11.1. Des messages légitimes sont signalés comme étant du [spam]

Des messages légitimes sont signalés comme étant du [spam] car ils ressemblent à du spam pour le filtre antispam de Bitdefender. Vous pouvez normalement régler ce problème en configurant le filtre Antispam de façon adaptée.

Bitdefender ajoute automatiquement les destinataires de vos e-mails à une Liste d'Amis. Les e-mails que vous recevez des contacts de la Liste d'Amis sont considérés comme légitimes. Ils ne sont pas vérifiés par le filtre antispam et ne sont donc jamais signalés comme étant du [spam].

La configuration automatique de la liste d'Amis n'empêche pas les erreurs de détection pouvant se produire dans les situations suivantes :

Vous recevez de nombreux e-mails commerciaux sollicités après vous être inscrit(e) sur plusieurs sites Internet. Dans ce cas, la solution est de ne pas ajouter les adresses e-mail des expéditeurs de ces messages à la liste d'Amis.

Une part importante des e-mails légitimes que vous recevez provient de personnes auxquelles vous n'avez jamais envoyé d'e-mail auparavant, telles que des clients, des partenaires commerciaux potentiels etc. D'autres solutions sont requises dans ce cas.

Si vous utilisez l'un des clients de messagerie dans lesquels Bitdefender s'intègre, indiquez les erreurs de détection.



Note
Bitdefender s'intègre dans la plupart des clients de messagerie via une barre d'outils antispam facile à utiliser. Pour une liste complète des clients de messagerie pris en charge, veuillez vous référer à *« Clients et protocoles de messagerie pris en charge »* (p. 119).

Ajouter des contacts à la Liste d'amis

Si vous utilisez un client de messagerie pris en charge, vous pouvez facilement ajouter les expéditeurs d'e-mails légitimes à la liste d'Amis. Suivez ces étapes :

1. Dans votre client de messagerie, sélectionnez un e-mail provenant de l'expéditeur que vous voulez ajouter à la liste d'Amis.
2. Cliquez sur le bouton **Ajouter un ami** de la barre d'outils antispam Bitdefender.
3. Il se peut qu'on vous demande de valider les adresses ajoutées à la liste d'Amis. Sélectionnez **Ne plus afficher ce message** et cliquez sur **OK**.

Les futurs messages provenant de cette adresse seront toujours dirigés vers votre boîte de réception quel que soit leur contenu.

Si vous utilisez un client de messagerie différent, vous pouvez ajouter des contacts à la liste d'Amis à partir de l'interface de Bitdefender. Suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Sous le module **Antispam**, sélectionnez **Gérer les amis**.

Une fenêtre de configuration s'affichera.

4. Tapez l'adresse e-mail à partir de laquelle vous souhaitez toujours recevoir les messages d'e-mail puis cliquez sur **Ajouter**.Vous pouvez ajouter autant d'adresses e-mail que vous le souhaitez.
5. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

Indiquer des erreurs de détection

Si vous utilisez un client de messagerie pris en charge, vous pouvez facilement corriger le filtre antispam (en indiquant quels e-mails n'auraient pas dû être signalés comme étant du [spam]). Cela contribue à améliorer considérablement l'efficacité du filtrage antispam.Suivez ces étapes :

1. Ouvrez votre client de messagerie.
2. Allez dans le dossier de courrier indésirable dans lequel les messages de spam sont placés.
3. Sélectionnez le message légitime considéré à tort comme étant du [spam] par Bitdefender.
4. Cliquez sur le bouton **Ajouter un ami** de la barre d'outils antispam Bitdefender pour ajouter l'expéditeur à la liste d'Amis.Il se peut que vous ayez besoin de cliquer sur **OK** pour valider.Les futurs messages provenant de cette adresse seront toujours dirigés vers votre boîte de réception quel que soit leur contenu.
5. Cliquez sur le bouton **Pas Spam** de la barre d'outils antispam de Bitdefender (généralement située dans la partie supérieure de la fenêtre du client de messagerie). Le message d'e-mail sera placé dans la boîte de réception.

32.11.2. De nombreux messages de spam ne sont pas détectés

Si vous recevez de nombreux messages de spam qui ne sont pas signalés comme étant du [spam], vous devez configurer le filtre antispam de Bitdefender pour améliorer son efficacité.

Essayez les solutions suivantes :

1. Si vous utilisez l'un des clients de messagerie dans lesquels Bitdefender s'intègre, indiquez les messages de spam non détectés.



Note

Bitdefender s'intègre dans la plupart des clients de messagerie via une barre d'outils antispam facile à utiliser.Pour une liste complète des clients de messagerie pris en charge, veuillez vous référer à *« Clients et protocoles de messagerie pris en charge »* (p. 119).

2. Ajouter des spammeurs à la liste des Spammeurs Les messages provenant d'adresses qui figurent dans la liste de Spammeurs seront automatiquement considérés comme étant du [spam].

Indiquer les messages de spam non détectés

Si vous utilisez un client de messagerie pris en charge, vous pouvez facilement indiquer quels e-mails auraient dû être détectés comme étant du spam. Cela contribue à améliorer considérablement l'efficacité du filtrage antispam.Suivez ces étapes :

1. Ouvrez votre client de messagerie.
2. Allez dans la boîte de Réception.
3. Sélectionnez les messages de spam non détectés.
4. Cliquez sur le bouton **Spam** de la barre d'outils antispam de Bitdefender (généralement située dans la partie supérieure de la fenêtre du client de messagerie). Ils sont immédiatement signalés comme étant du [spam] et déplacés vers le dossier du courrier indésirable.

Ajouter des spammeurs à la Liste des Spammeurs

Si vous utilisez un client de messagerie pris en charge, vous pouvez facilement ajouter les expéditeurs de spam à la liste de Spammeurs. Suivez ces étapes :

1. Ouvrez votre client de messagerie.
2. Allez dans le dossier de courrier indésirable dans lequel les messages de spam sont placés.
3. Sélectionnez les messages signalés comme étant du [spam] par Bitdefender.
4. Cliquez sur le bouton **Ajouter Spammeur** de la barre d'outils antispam Bitdefender.

5. Il se peut qu'on vous demande de valider les adresses ajoutées à la liste de Spammeurs. Sélectionnez **Ne plus afficher ce message** et cliquez sur **OK**.

Si vous utilisez un autre client de messagerie, vous pouvez ajouter manuellement des spammeurs à la liste des Spammeurs à partir de l'interface de Bitdefender. Cela s'avère utile lorsque vous avez reçu plusieurs e-mails de spam provenant de la même adresse e-mail. Suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Sous le module **Antispam**, sélectionnez **Gérer spammeurs**.

   Une fenêtre de configuration s'affichera.
4. Tapez l'adresse e-mail du spammeur puis cliquez sur **Ajouter**.Vous pouvez ajouter autant d'adresses e-mail que vous le souhaitez.
5. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

32.11.3. Le filtre antispam ne détecte aucun message de spam.

Si aucun message de spam n'est signalé comme étant du [spam], il se peut qu'il y ait un problème avec le filtre Antispam de Bitdefender.Avant d'essayer de régler ce problème, assurez-vous qu'il n'est pas causé par l'une des situations suivantes :

La protection antispam pourrait être désactivée. Pour vérifier l'état de la protection antispam, ouvrez la fenêtre Bitdefender, accédez au panneau **Protection**, cliquez sur le module **Antispam** et vérifiez le bouton dans la fenêtre **Configuration**.

Si l'Antispam est désactivé, il s'agit de la cause de votre problème.Cliquez sur le bouton pour activer votre protection antispam.

La protection Bitdefender Antispam est disponible seulement pour les clients de messagerie configurés pour recevoir des e-mails via le protocole POP3.Cela signifie que :

Les e-mails reçus via des services de webmail (tels que Yahoo, Gmail, Hotmail ou d'autres) ne font pas l'objet d'une analyse antispam de la part de Bitdefender.

Si votre client de messagerie est configuré pour recevoir des e-mails en utilisant un protocole autre que POP3 (par exemple IMAP4), vos e-mails ne seront pas analysés par Bitdefender Antispam.



Note

POP3 est l'un des protocoles les plus utilisés pour télécharger des e-mails à partir d'un serveur de messagerie. Si vous ne connaissez pas le protocole que votre client de messagerie utilise pour télécharger des e-mails, posez la question à la personne ayant configuré votre client de messagerie.

Bitdefender Internet Security 2015 n'analyse pas le trafic POP3 de Lotus Notes.

Une solution possible consiste à réparer ou à réinstaller le produit. Il est toutefois recommandé de contacter Bitdefender pour obtenir de l'assistance, comme cela est décrit dans la section « *Demander de l'aide* » (p. 233).

32.12. La fonctionnalité saisie automatique de mon Portefeuille ne fonctionne pas

Vous avez enregistré vos identifiants en ligne dans votre Bitdefender Wallet et avez remarqué que la saisie automatique ne fonctionne pas. Ce problème sse produit généralement lorsque l'extension de Bitdefender Wallet n'est pas installée dans votre navigateur.

Pour résoudre cette situation, suivez ces étapes :

Dans **Internet Explorer :**

1. Ouvrez Internet Explorer.
2. Cliquez sur Outils.
3. Cliquez sur Gérer les modules.
4. Cliquez sur Barres d'outils et Extensions.
5. Pointez sur **Bitdefender Wallet** et cliquez sur Permettre.

Dans **Mozilla Firefox :**

1. Ouvrez Mozilla Firefox.
2. Cliquez sur Outils.
3. Cliquez sur Modules.

4. Cliquez sur Extensions.
5. Pointez sur **Bitdefender Wallet** et cliquez sur Permettre.

Dans **Google Chrome :**

1. Ouvrez Google Chrome.
2. Allez sur l'icône du Menu.
3. Cliquez sur Paramètres.
4. Cliquez sur Extensions.
5. Pointez sur **Bitdefender Wallet** et cliquez sur Permettre.



Note
Le module sera activé une fois que vous aurez redémarré votre navigateur Web.

Vérifiez maintenant que la fonctionnalité de saisie automatique de Portefeuille fonctionne pour vos comptes en ligne.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Demander de l'aide* » (p. 233).

32.13. La désinstallation de Bitdefender a échoué

Si vous souhaitez supprimer votre produit Bitdefender et remarquez que le processus se bloque ou que le système se fige, cliquez sur **Annuler** pour annuler l'action. Si cela ne fonctionne pas, redémarrez le système.

Lorsque la désinstallation échoue, certaines clés de registre et fichiers de Bitdefender peuvent demeurer sur votre système. De tels restes peuvent empêcher une nouvelle installation de Bitdefender. Ils peuvent aussi affecter la performance du système et sa stabilité.

Afin de désinstaller complètement Bitdefender de votre système, procédez comme suit :

Dans **Windows XP**:

1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Ajout/Suppression de programmes**.
2. Localisez **Bitdefender Internet Security 2015** et sélectionnez **Supprimer**.
3. Cliquez sur **Supprimer** dans la fenêtre qui s'affiche.

4. Vous disposez à cette étape des options suivantes :

   Je souhaite le réinstaller - désinstallera complètement Bitdefender. Bitdefender 60-Second Virus Scanner ne sera pas installé.

   Je souhaite le désinstaller définitivement - désinstallera complètement Bitdefender. Bitdefender 60-Second Virus Scanner sera installé sur votre système pour vous protéger contre les malwares.

   Sélectionnez l'option souhaitée et cliquez sur **Suivant**.

5. Attendez la fin du processus de désinstallation et puis redémarrez votre système.

Dans **Windows Vista** et **Windows 7**:

1. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.
2. Localisez **Bitdefender Internet Security 2015** et sélectionnez **Désinstaller**.
3. Cliquez sur **Supprimer** dans la fenêtre qui s'affiche.
4. Vous disposez à cette étape des options suivantes :

   Je souhaite le réinstaller - désinstallera complètement Bitdefender. Bitdefender 60-Second Virus Scanner ne sera pas installé.

   Je souhaite le désinstaller définitivement - désinstallera complètement Bitdefender. Bitdefender 60-Second Virus Scanner sera installé sur votre système pour vous protéger contre les malwares.

   Sélectionnez l'option souhaitée et cliquez sur **Suivant**.

5. Attendez la fin du processus de désinstallation et puis redémarrez votre système.

Dans **Windows 8** :

1. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.
2. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.

3. Localisez **Bitdefender Internet Security 2015** et sélectionnez **Désinstaller**.
4. Cliquez sur **Supprimer** dans la fenêtre qui s'affiche.
5. Vous disposez à cette étape des options suivantes :

   Je souhaite le réinstaller - désinstallera complètement Bitdefender. Bitdefender 60-Second Virus Scanner ne sera pas installé.

   Je souhaite le désinstaller définitivement - désinstallera complètement Bitdefender. Bitdefender 60-Second Virus Scanner sera installé sur votre système pour vous protéger contre les malwares.

   Sélectionnez l'option souhaitée et cliquez sur **Suivant**.
6. Attendez la fin du processus de désinstallation et puis redémarrez votre système.



Note

Bitdefender 60-Second Virus Scanner est une application gratuite qui utilise une technologie d'analyse dans le cloud pour détecter les programmes malveillants et les menaces en moins de 60 secondes.

32.14. Mon système ne démarre pas après l'installation de Bitdefender

Si vous venez d'installer Bitdefender et ne pouvez plus redémarrer votre système en mode normal, il peut y avoir plusieurs raisons à ce problème.

Cela est sans doute dû à une installation précédente de Bitdefender qui n'a pas été désinstallée correctement ou à une autre solution de sécurité toujours présente sur le système.

Voici comment faire face à chaque situation :

Vous aviez Bitdefender et vous ne l'avez pas désinstallé correctement.

Pour résoudre cela, suivez ces étapes :

1. Redémarrez votre système et entrez en Mode sans échec. Pour savoir comment faire cela, consultez *« Comment redémarrer en mode sans échec ? »* (p. 88).
2. Désinstallez Bitdefender de votre système :

Dans **Windows XP**:

a. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Ajout/Suppression de programmes**.

b. Localisez **Bitdefender Internet Security 2015** et sélectionnez **Supprimer**.

c. Cliquez sur **Supprimer** dans la fenêtre qui apparaît puis sélectionnez **Je souhaite le réinstaller**.

d. Cliquez sur **Suivant** pour continuer.

e. Décochez l'option **Installer Bitdefender 60-Second Virus Scanner** et cliquez sur **Suivant**.

f. Patientez jusqu'à la fin du processus de désinstallation.

g. Redémarrez votre système en mode normal.

Dans **Windows Vista** et **Windows 7**:

a. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.

b. Localisez **Bitdefender Internet Security 2015** et sélectionnez **Désinstaller**.

c. Cliquez sur **Supprimer** dans la fenêtre qui apparaît puis sélectionnez **Je souhaite le réinstaller**.

d. Cliquez sur **Suivant** pour continuer.

e. Décochez l'option **Installer Bitdefender 60-Second Virus Scanner** et cliquez sur **Suivant**.

f. Patientez jusqu'à la fin du processus de désinstallation.

g. Redémarrez votre système en mode normal.

Dans **Windows 8** :

a. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.

b. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.

c. Localisez **Bitdefender Internet Security 2015** et sélectionnez **Désinstaller**.

d. Cliquez sur **Supprimer** dans la fenêtre qui apparaît puis sélectionnez **Je souhaite le réinstaller**.

e. Cliquez sur **Suivant** pour continuer.

f. Décochez l'option **Installer Bitdefender 60-Second Virus Scanner** et cliquez sur **Suivant**.

g. Patientez jusqu'à la fin du processus de désinstallation.

h. Redémarrez votre système en mode normal.

3. Réinstallez votre produit Bitdefender.

Vous aviez une autre solution de sécurité auparavant et vous ne l'avez pas désinstallée correctement.

Pour résoudre cela, suivez ces étapes :

1. Redémarrez votre système et entrez en Mode sans échec. Pour savoir comment faire cela, consultez *« Comment redémarrer en mode sans échec ? »* (p. 88).

2. Désinstallez l'autre solution de sécurité de votre système :

   Dans **Windows XP**:

   a. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Ajout/Suppression de programmes**.

   b. Patientez quelques instants, jusqu'à ce que la liste des logiciels installés s'affiche.

   c. Trouvez le nom du programme que vous souhaitez supprimer, puis sélectionnez **Supprimer**.

   d. Attendez la fin du processus de désinstallation et puis redémarrez votre système.

   Dans **Windows Vista** et **Windows 7**:

   a. Cliquez sur **Démarrer**, allez dans **Panneau de configuration** et double-cliquez sur **Programmes et fonctionnalités**.

   b. Patientez quelques instants, jusqu'à ce que la liste des logiciels installés s'affiche.

c. Trouvez le nom du programme que vous souhaitez supprimer, puis sélectionnez **Supprimer**.

d. Attendez la fin du processus de désinstallation et puis redémarrez votre système.

Dans **Windows 8** :

a. Dans l'écran d'accueil Windows, localisez le **Panneau de configuration** (vous pouvez par exemple taper « Panneau de configuration » directement dans l'écran d'accueil) puis cliquez sur son icône.

b. Cliquez sur **Désinstaller un programme** ou sur **Programmes et fonctionnalités**.

c. Patientez quelques instants, jusqu'à ce que la liste des logiciels installés s'affiche.

d. Trouvez le nom du programme que vous souhaitez supprimer, puis sélectionnez **Supprimer**.

e. Attendez la fin du processus de désinstallation et puis redémarrez votre système.

Afin de désinstaller correctement les autres logiciels, allez sur leur site Internet et exécutez leur outil de désinstallation, ou contactez-les directement afin qu'ils vous indiquent la procédure de désinstallation.

3. Redémarrez votre système en mode normal et réinstallez Bitdefender.

Vous avez déjà suivi les étapes ci-dessus et la situation n'est pas résolue.

Pour résoudre cela, suivez ces étapes :

1. Redémarrez votre système et entrez en Mode sans échec. Pour savoir comment faire cela, consultez *« Comment redémarrer en mode sans échec ? »* (p. 88).
2. Utilisez l'option Restauration du Système de Windows pour restaurer l'ordinateur à une date antérieure à l'installation du produit Bitdefender. Pour savoir comment faire cela, consultez *« Comment utiliser la restauration du système dans Windows ? »* (p. 87).
3. Redémarrez le système en mode normal et contactez les représentants de notre soutien technique pour obtenir de l'aide, comme indiqué dans la section *« Demander de l'aide »* (p. 233).

33. SUPPRESSION DES MALWARES DE VOTRE SYSTÈME

Les malwares peuvent affecter votre système de nombreuses manières et l'approche de Bitdefender dépend du type d'attaque de malware.Les virus changeant souvent de comportement, il est difficile de définir leur comportement et leurs actions.

Il s'agit des situations où Bitdefender ne peut supprimer automatiquement l'infection de malwares de votre système. Dans ce cas, votre intervention est nécessaire.

Si vous ne parvenez pas à trouver votre problème ici, ou si les solutions présentées ne le résolvent pas, vous pouvez contacter les représentants du soutien technique Bitdefender comme indiqué dans le chapitre « *Demander de l'aide* » (p. 233).

33.1. Mode de Secours de Bitdefender

Le **Mode de secours** est une fonctionnalité de Bitdefender qui vous permet d'analyser et de désinfecter toutes les partitions de votre disque dur hors de votre système d'exploitation.

Une fois Bitdefender Internet Security 2015 installé, le Mode de Secours peut être utilisé même si vous ne pouvez plus démarrer sous Windows.

Démarrer votre système en mode de secours

Vous pouvez entrer en mode de secours de l'une des deux façons suivantes :

À partir de la fenêtre Bitdefender

Pour entrer en Mode de Secours directement à partir de Bitdefender, suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Accédez au panneau **Protection**.
3. Sous le module **Antivirus**, sélectionnez **Mode de secours**.

   Une fenêtre de confirmation s'affichera. Cliquez sur **Oui** pour redémarrer votre ordinateur.
4. Après le redémarrage de l'ordinateur, un menu apparaîtra vous demandant de sélectionner un système d'exploitation. Sélectionnez **Mode de Secours de Bitdefender** et appuyez sur la touche **Entrée** pour démarrer dans un environnement Bitdefender vous permettant de nettoyer votre partition Windows.
5. Si cela vous est demandé, cliquez sur **Entrée** et sélectionnez la résolution d'écran la plus proche de celle que vous utilisez habituellement. Puis, cliquez de nouveau sur **Entrée**.

   Le Mode de Secours de Bitdefender se chargera dans quelques instants.

Démarrez votre ordinateur directement en mode de secours

Si Windows ne démarre plus, vous pouvez démarrer directement votre ordinateur en Mode de Secours de Bitdefender en suivant les étapes ci-dessous:



Note

Cette méthode n'est pas disponible pour les ordinateurs fonctionnant sous Windows XP.

1. Démarrez / redémarrez votre ordinateur et appuyez sur la touche **espace** de votre clavier avant que n'apparaisse le logo Windows.

2. Un menu apparaîtra vous demandant de sélectionner un système d'exploitation à démarrer. Cliquez sur **ONGLET** pour vous rendre dans la zone d'outils. Sélectionnez **Image de Secours de Bitdefender** et appuyez sur la touche **Entrée** pour démarrer dans un environnement Bitdefender vous permettant de nettoyer votre partition Windows.
3. Si cela vous est demandé, cliquez sur **Entrée** et sélectionnez la résolution d'écran la plus proche de celle que vous utilisez habituellement. Puis, cliquez de nouveau sur **Entrée**.

   Le Mode de Secours de Bitdefender se chargera dans quelques instants.

Analyser votre système en mode de secours

Pour analyser votre système en mode de secours, procédez comme suit :

1. Entrez en mode de secours, comme indiqué dans « Démarrer votre système en mode de secours » (p. 222).
2. Le logo Bitdefender apparaîtra et les moteurs antivirus commenceront à être copiés.
3. Une fenêtre d'accueil apparaîtra. Cliquez sur **Continuer**.
4. Une mise à jour des signatures antivirus a démarré.
5. Une fois la mise à jour terminée, la fenêtre du Scanner Antivirus à la demande Bitdefender s'affiche.
6. Cliquez sur **Analyser**, sélectionnez la cible de l'analyse dans la fenêtre qui s'affiche et cliquez sur **Ouvrir** pour lancer l'analyse.

   Nous vous recommandons l'analyse de la totalité de votre partition Windows.

   Note
   En mode de secours, les noms de partitions sont de type Linux. Des partitions de disque apparaîtront, `sda1` correspondant probablement à la partition de type Windows `(C:)`, `sda2` correspondant à `(D:)`, etc.

7. Patientez jusqu'à la fin de l'analyse. Si un malware est détecté, suivez les instructions pour supprimer la menace.

8. Pour quitter le mode de secours, faites un clic droit sur une zone vide du bureau, sélectionnez **Quitter** dans le menu qui apparaît puis choisissez de redémarrer ou d'éteindre l'ordinateur.

33.2. Que faire lorsque Bitdefender détecte des virus sur votre ordinateur ?

Il est possible que vous découvriez qu'un virus se trouve sur votre ordinateur de l'une des manières suivantes :

Vous avez analysé votre ordinateur et Bitdefender y a détecté des éléments infectés.

Une alerte de virus vous informe que Bitdefender a bloqué un ou plusieurs virus sur votre ordinateur.

Dans de telles situations, mettez à jour Bitdefender pour vous assurer de disposer des dernières signatures de malwares puis exécutez une analyse du système.

Dès que l'analyse du système est terminée, sélectionnez l'action souhaitée à appliquer aux éléments infectés (Désinfecter, Supprimer, Quarantaine).



Avertissement

Si vous pensez que le fichier fait partie du système d'exploitation Windows ou qu'il ne s'agit pas d'un fichier infecté, ne suivez pas ces étapes et contactez le Service Client de Bitdefender dès que possible.

Si l'action sélectionnée ne peut être appliquée et que le journal d'analyse révèle une infection qui ne peut être supprimée, vous devez supprimer le(s) fichier(s) manuellement :

La première méthode peut être utilisée en mode normal :

1. Désactivez la protection antivirus en temps réel de Bitdefender :
   a. Ouvrez la fenêtre de Bitdefender.
   b. Accédez au panneau **Protection**.
   c. Cliquez sur le module **Antivirus**.
   d. Dans la fenêtre **Antivirus**, sélectionnez l'onglet **Résident**.
   e. Cliquez sur le bouton pour désactiver l'**Analyse à l'accès**.

2. Afficher les objets masqués dans Windows. Pour savoir comment faire cela, consultez *« Comment afficher des objets cachés dans Windows ? »* (p. 85).
3. Accédez à l'emplacement du fichier infecté (consultez le journal d'analyse), puis supprimez-le.
4. Activez la protection antivirus en temps réel de Bitdefender.

Si la première méthode ne parvient pas à supprimer l'infection, suivez ces étapes :

1. Redémarrez votre système et entrez en Mode sans échec. Pour savoir comment faire cela, consultez *« Comment redémarrer en mode sans échec ? »* (p. 88).
2. Afficher les objets masqués dans Windows. Pour savoir comment faire cela, consultez *« Comment afficher des objets cachés dans Windows ? »* (p. 85).
3. Accédez à l'emplacement du fichier infecté (consultez le journal d'analyse), puis supprimez-le.
4. Redémarrez votre système et entrez en mode normal.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section *« Demander de l'aide »* (p. 233).

33.3. Comment nettoyer un virus dans une archive ?

Une archive est un fichier ou un ensemble de fichiers compressés sous un format spécial pour réduire l'espace nécessaire sur le disque pour stocker les fichiers.

Certains de ces formats sont des formats ouverts, permettant ainsi à Bitdefender de les analyser, puis de mener les actions appropriées pour les supprimer.

D'autres formats d'archive sont fermés partiellement ou totalement, et Bitdefender peut uniquement détecter la présence de virus dans ceux-ci, mais n'est pas capable de mener d'autres actions.

Si Bitdefender indique qu'un virus a été détecté dans une archive et qu'aucune action n'est disponible, cela signifie qu'il n'est pas possible de supprimer le virus en raison de restrictions sur les paramètres d'autorisation de l'archive.

Voici comment nettoyer un virus stocké dans une archive :

1. Identifiez l'archive où se trouve le virus en réalisant une analyse du système.
2. Désactivez la protection antivirus en temps réel de Bitdefender :
   a. Ouvrez la fenêtre de Bitdefender.
   b. Accédez au panneau **Protection**.
   c. Cliquez sur le module **Antivirus**.
   d. Dans la fenêtre **Antivirus**, sélectionnez l'onglet **Résident**.
   e. Cliquez sur le bouton pour désactiver l'**Analyse à l'accès**.
3. Rendez-vous à l'emplacement de l'archive et décompressez-la à l'aide d'une application d'archivage, comme WinZip.
4. Identifier le fichier infecté et le supprimer.
5. Supprimez l'archive d'origine afin de vous assurer que l'infection est totalement supprimée.
6. Recompressez les fichiers dans une nouvelle archive à l'aide d'une application d'archivage, comme WinZip.
7. Activez la protection antivirus en temps réel de Bitdefender et exécutez une analyse complète du système afin de vous assurer qu'aucune autre infection n'est présente sur le système.



Note
Il est important de noter qu'un virus contenu dans une archive ne représente pas de menace immédiate pour votre système, puisque, pour infecter votre système, le virus doit être décompressé et exécuté.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Demander de l'aide* » (p. 233).

33.4. Comment nettoyer un virus dans une archive de messagerie ?

Bitdefender permet également de repérer les virus dans les bases de données d'e-mails et les archives d'e-mails stockées sur le disque.

Il est parfois nécessaire d'identifier le message infecté à l'aide des informations du rapport d'analyse, et de le supprimer manuellement.

Voici comment nettoyer un virus stocké dans une archive de messagerie électronique :

1. Analysez la base de données des e-mails avec Bitdefender.
2. Désactivez la protection antivirus en temps réel de Bitdefender :
   a. Ouvrez la fenêtre de Bitdefender.
   b. Accédez au panneau **Protection**.
   c. Cliquez sur le module **Antivirus**.
   d. Dans la fenêtre **Antivirus**, sélectionnez l'onglet **Résident**.
   e. Cliquez sur le bouton pour désactiver l'**Analyse à l'accès**.
3. Ouvrez le rapport d'analyse et utilisez les informations d'identification (Sujet, Expéditeur, Destinataire) des messages infectés pour les localiser dans le client de messagerie.
4. Supprimez les messages infectés.La plupart des clients de messagerie placent les messages supprimés dans un dossier de récupération permettant de les restaurer.Il est recommandé de vous assurer que le message a été supprimé également dans ce dossier de récupération.
5. Compressez le dossier contenant le message infecté.

   Dans Outlook Express :Dans le menu Fichier, cliquez sur Dossier, puis sur Compacter tous les dossiers.

   Dans Microsoft Outlook 2007 :Dans le menu Fichier, cliquez sur Gestion des fichiers de données.Sélectionnez les dossiers de fichiers personnels (.pst) que vous souhaitez compresser, puis cliquez sur Configuration.Cliquez sur Compresser.

   Dans Microsoft Outlook 2010 / 2013 :Dans le menu Fichier, cliquez sur Infos puis sur Paramètres du compte (Ajouter et supprimer des comptes ou modifier les paramètres de connexion existants).Cliquez ensuite sur Fichier de données, sélectionnez les fichiers des dossiers personnels (.pst) que vous souhaitez compacter puis cliquez sur Paramètres.Cliquez sur Compresser.
6. Activez la protection antivirus en temps réel de Bitdefender.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section « *Demander de l'aide* » (p. 233).

33.5. Que faire si je suspecte un fichier d'être dangereux ?

Vous pouvez suspecter qu'un fichier de votre système est dangereux, même si votre produit Bitdefender ne l'a pas détecté.

Pour vérifier que votre système est protégé, suivez ces étapes :

1. Exécuter une **Analyse du Système** avec Bitdefender. Pour savoir comment faire cela, reportez-vous à *« Comment analyser mon système ? »* (p. 62).
2. Si le résultat de l'analyse n'indique pas d'infection, mais que vous avez encore des doutes et souhaitez vérifier le fichier, contactez les représentants de notre soutien technique afin que nous puissions vous aider.

   Pour savoir comment faire cela, consultez *« Demander de l'aide »* (p. 233).

33.6. Comment nettoyer les fichiers infectés du dossier System Volume Information ?

Le dossier System Volume Information est une zone du disque dur créée par le système d'exploitation et utilisée par Windows pour stocker des informations critiques relatives à la configuration du système.

Les moteurs de Bitdefender permettent de détecter tout fichier infecté stocké par le System Volume Information mais, étant donné que c'est une zone protégée, il est possible qu'il ne puisse pas les supprimer.

Les fichiers infectés détectés dans les dossiers Restauration du Système apparaîtront dans le journal d'analyse comme suit :

?:\System Volume Information_restore{B36120B2-BA0A-4E5D-...

Pour supprimer complètement et immédiatement le ou les fichiers infectés dans la banque de données, désactivez, puis réactivez la fonction restauration du système.

Lorsque la restauration du système est désactivée, tous les points de restauration sont supprimés.

Lorsque la restauration du système est réactivée, de nouveaux points de restauration sont créés en fonction des besoins de la planification et des événements.

Pour désactiver la restauration du système, procédez comme suit :

Pour Windows XP :

1. Suivez ce chemin : **Démarrer** → **Tous les programmes** → **Accessoires** → **Outils système** → **Restauration du système**
2. Cliquez sur **Paramètres de restauration du système** situé à gauche de la fenêtre.
3. Cochez la case **Désactiver la Restauration du Système** sur tous les lecteurs et cliquez sur **Appliquer**.
4. Lorsque l'on vous informe que tous les points de restauration existants seront supprimés, cliquez sur **Oui** pour continuer.
5. Pour activer la restauration du système, décochez la case **Désactiver la Restauration du Système** sur tous les lecteurs, et cliquez sur **Appliquer**.

Pour Windows Vista :

1. Suivez ce chemin : **Démarrer** → **Panneau de configuration** → **Système et maintenance** → **Système**
2. Dans le volet gauche, cliquez sur **Protection du système**.

   Si l'on vous demande un mot de passe administrateur ou une confirmation, saisissez le mot de passe ou confirmez-le.
3. Pour désactiver la restauration du système, décochez les cases correspondant à chaque lecteur et cliquez sur **OK**.
4. Pour activer la restauration du système, cochez les cases correspondant à chaque lecteur et cliquez sur **OK**.

Pour Windows 7 :

1. Cliquez sur **Démarrer**, faites un clic droit sur **Ordinateur**, puis cliquez sur **Propriétés**.
2. Cliquez sur le lien **Protection du système** dans le volet gauche.
3. Dans les options **Protection du système**, sélectionnez chaque lettre des lecteurs, puis cliquez sur **Configurer**.
4. Sélectionnez **Désactiver la protection du système** et cliquez sur **Appliquer**.
5. Cliquez sur **Supprimer**, puis sur **Continuer** lorsqu'on vous le demande et enfin sur **OK**.

Pour Windows 8 :

1. Dans l'écran d'accueil Windows, localisez l'**Ordinateur** (vous pouvez par exemple taper « Ordinateur » directement dans l'écran d'accueil) puis cliquez sur son icône.
2. Cliquez sur le lien **Protection du système** dans le volet gauche.
3. Dans les options **Protection du système**, sélectionnez chaque lettre des lecteurs, puis cliquez sur **Configurer**.
4. Sélectionnez **Désactiver la protection du système** et cliquez sur **Appliquer**.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support Bitdefender comme indiqué dans la section *« Demander de l'aide »* (p. 233).

33.7. Que sont les fichiers protégés par mot de passe du journal d'analyse ?

Il ne s'agit que d'une notification qui indique que Bitdefender a détecté que ces fichiers sont soit protégés par un mot de passe soit par une forme de cryptage.

Les éléments protégés par un mot de passe sont généralement :

Fichiers appartenant à une autre solution de sécurité.

Fichiers appartenant au système d'exploitation.

Afin que le contenu soit analysé, ces fichiers auront besoin d'être extraits ou décryptés.

Si ce contenu était extrait, le moteur d'analyse en temps réel de Bitdefender l'analyserait automatiquement pour que votre ordinateur reste protégé. Si vous souhaitez analyser ces fichiers avec Bitdefender, vous devez contacter le fabricant du produit afin d'obtenir plus d'informations sur ces fichiers.

Nous vous recommandons d'ignorer ces fichiers car ils ne constituent pas une menace pour votre système.

33.8. Que sont les éléments ignorés du journal d'analyse ?

Tous les fichiers apparaissant comme ignorés dans le rapport d'analyse sont sains.

Pour de meilleures performances, Bitdefender n'analyse pas les fichiers n'ayant pas été modifiés depuis la dernière analyse.

33.9. Que sont les fichiers ultra-compressés du journal d'analyse ?

Les éléments ultra-compressés sont des éléments qui n'ont pas pu être extraits par le moteur d'analyse ou des éléments dont le temps de décryptage aurait été trop long et aurait rendu le système instable.

Surcompressé signifie que Bitdefender a ignoré l'analyse dans cette archive car sa décompression consommait trop de ressources système. Le contenu sera analysé à l'accès en temps réel si nécessaire.

33.10. Pourquoi Bitdefender a-t-il supprimé automatiquement un fichier infecté ?

Si un fichier infecté est détecté, Bitdefender tente automatiquement de le désinfecter.Si la désinfection échoue, le fichier est placé en quarantaine afin de contenir l'infection.

Pour certains types de malware, la désinfection n'est pas possible, car le fichier détecté est entièrement malveillant. Dans ce cas, le fichier infecté est supprimé du disque.

C'est généralement le cas avec les fichiers d'installation qui sont téléchargés depuis des sites non fiables.Si vous vous trouvez dans une telle situation, téléchargez le fichier d'installation sur le site Web du fabricant ou sur un autre site de confiance.

NOUS CONTACTER

34. DEMANDER DE L'AIDE

Bitdefender fournit à ses clients une aide hors pair, rapide et efficace. Si vous rencontrez le moindre problème ou si vous avez des questions sur votre produit Bitdefender, vous pouvez utiliser plusieurs ressources en ligne pour trouver rapidement une solution ou une réponse. Vous pouvez également contacter l'équipe du Service Client de Bitdefender. Nos membres du support technique répondront à vos questions aussi rapidement que possible et vous fourniront l'assistance dont vous avez besoin.

La section *« Résoudre les problèmes les plus fréquents »* (p. 196) fournit les informations nécessaires concernant les problèmes les plus fréquents que vous pouvez rencontrer lors de l'utilisation de ce produit.

Si vous ne trouvez pas de réponse à votre question dans les ressources fournies, vous pouvez nous contacter directement :

« Contactez-nous directement à partir de votre produit Bitdefender » (p. 233)

« Contactez-nous via notre Centre de Support en ligne » (p. 234)

Important

Pour contacter le Service Client de Bitdefender, vous devez enregistrer votre produit Bitdefender. Pour plus d'informations, consultez *« Activer Bitdefender »* (p. 39).

Contactez-nous directement à partir de votre produit Bitdefender

Si vous disposez d'une connexion Internet, vous pouvez contacter l'assistance de Bitdefender directement à partir de l'interface du produit.

Suivez ces étapes :

1. Ouvrez la fenêtre de Bitdefender.
2. Cliquez sur l'icône en haut de la fenêtre et sélectionnez **Aide & Support** dans le menu déroulant.
3. Vous disposez des options suivantes :

    Documentation du produit

Accédez à notre base de données et recherchez les informations nécessaires.

Contacter le Support

Utilisez le bouton **Contacter le Support** pour lancer l'Outil Support de Bitdefender et contacter le Support Client. Vous pouvez naviguer dans l'assistant à l'aide du bouton **Suivant**. Pour quitter l'assistant, cliquez sur **Annuler**.

a. Cochez la case d'accord et cliquez sur **Suivant**.

b. Compléter le formulaire de soumission avec les données nécessaires :

   i. Saisissez votre adresse e-mail.

   ii. Indiquez votre nom complet.

   iii. Décrivez le problème que vous avez rencontré.

   iv. Sélectionnez l'option **Essayer de reproduire le problème avant la soumission** si vous rencontrez un problème avec le produit. Poursuivez avec les étapes requises.

c. Veuillez patienter pendant quelques minutes pendant que Bitdefender recueille les informations sur le produit. Ces informations aideront nos ingénieurs à trouver une solution à votre problème.

d. Cliquez sur **Terminer** pour envoyer les informations au Service Client de Bitdefender. Nous vous contacterons dès que possible.

Contactez-nous via notre Centre de Support en ligne

Si vous ne parvenez pas à accéder aux informations nécessaires à l'aide du produit Bitdefender, consultez notre Centre de Support en ligne :

1. Allez à http://www.bitdefender.fr/support/consumer.html.

   Le Centre de Support de Bitdefender contient de nombreux articles apportant des solutions aux problèmes liés à Bitdefender.

2. Utilisez la barre de recherche en haut de la fenêtre pour trouver des articles susceptibles d'apporter une solution à votre problème. Pour effectuer une recherche, saisissez simplement un terme dans la barre de recherche et cliquez sur **Rechercher**.

3. Consultez les articles et les documents pertinents et essayez les solutions proposées.

4. Si la solution ne règle pas votre problème, allez dans

   http://www.bitdefender.fr/support/nous-contacter.htmlet contactez nos représentants du support.

34.1. Support Technique Profil Technology / Bitdefender

Centre d'Assistance des Laboratoires Technologiques et Scientifiques

Les Laboratoires de Profil Technology et de Bitdefender assurent un niveau d'assistance sur tous les produits maintenus par l'équipe de développement. La résolution d'un problème peut nous amener à vous proposer de mettre gratuitement à niveau la version de votre produit.

Ce service offre une assistance pour les questions ou problèmes liés à des applications courantes pour l'utilisateur final ou les entreprises, telles que :

Des configurations personnalisées des produits Bitdefender.
Des conseils de prise en main en monoposte ou en relation avec des réseaux simples.
Des problèmes techniques après l'installation des produits Bitdefender.
Des aides afin de contrer les activités de codes malicieux présents sur un système.
L'accès à notre site internet de maintenance personnalisée et de FAQ en ligne 24h/24 et 7j/7 : http://www.bitdefender.fr/site/KnowledgeBase/supportCenter/.
L'accès aux informations des centres de support internationaux, qui permettent de gérer les situations par chat online – Accessible 7j/7 – 365j/an. Pour y accéder, veuillez saisir l'adresse ci-dessous dans votre navigateur : http://www.bitdefender.fr/site/KnowledgeBase/getSupport/. Attention : ce module est un service international, assuré majoritairement en Anglais.

Assistance téléphonique :

Les Laboratoires Profil Technology et Bitdefender mettent en oeuvre tous les efforts commercialement envisageables pour maintenir l'accès à l'assistance téléphonique de ce service, pendant les heures ouvrées locales du lundi au vendredi, sauf pendant les jours fériés.

Accès téléphoniques aux Laboratoires Profil Technology et Bitdefender :

Pour la France et les DOM-TOM : 0892 561 161 (0.34 euros / minute)
Pour la Belgique : 070 35 83 04
Pour la Suisse : 0900 000 118 (0,60 FS / minute)

Avant de nous appeler, munissez-vous :

du numéro de licence du produit Bitdefender. Communiquez le à un de nos analystes afin qu'il vérifie votre niveau d'assistance.
de la version actuelle du système d'exploitation.
des informations sur les marques et modèles de tous les périphériques et des logiciels chargés en mémoire ou utilisés.

En cas d'infection, l'analyste pourra demander une liste d'informations techniques à fournir ainsi que certains fichiers, qui pourront être nécessaires à son diagnostic.

Lorsqu'un analyste vous le demande, précisez les messages d'erreurs reçus et le moment où ils apparaissent, les activités qui ont précédées le message d'erreur et les démarches déjà entreprises pour résoudre le problème.

L'analyste suivra une procédure de dépannage stricte afin de tenter de diagnostiquer le problème.

Le Service n'inclut pas les éléments suivants :

Ce service d'assistance ne comprend pas les applications, les installations, la désinstallation, le transfert, la maintenance préventive, la formation, l'administration à distance ou configurations logicielles autres que celles spécifiquement notifiées par l'analyste des Laboratoires Profil Technology et Bitdefender lors de l'intervention.
L'installation, le paramétrage, l'optimisation et la configuration en réseau ou à distance d'applications n'entrant pas dans le cadre de l'assistance actuelle.
Sauvegarde des logiciels/données. Il incombe au Client d'effectuer une sauvegarde de toutes les données, des logiciels et des programmes existants sur les systèmes d'information pris en charge avant toute prestation de service par Profil Technology et de Bitdefender.

Profil Technology ou Bitdefender NE PEUVENT ÊTRE TENUS RESPONSABLE DE LA PERTE OU DE LA RÉCUPÉRATION DE DONNÉES, DE PROGRAMMES, OU DE LA PRIVATION DE JOUISSANCE DES SYSTÈME(S) OU DU RÉSEAU.

Les conseils sont strictement limités aux questions demandées et basées sur les informations fournies par le client. Les problèmes et les solutions peuvent dépendre de la nature de l'environnement du système et d'une variété d'autres paramètres qui sont inconnus à Profil Technology ou Bitdefender. Par conséquent, Profil Technology ou Bitdefender ne peuvent en aucun cas être tenus responsable de dommages résultant de l'utilisation de ces informations.

Il est possible que l'état du système sur lequel les produits Bitdefender doivent être installés soit instable (infection préalable, installation d'antivirus ou solutions de sécurité multiples, etc.). Dans ces cas précis, il est possible que l'analyste vous propose une prestation de maintenance auprès de votre revendeur avant de pouvoir régler votre problème.

Les informations techniques peuvent changer lorsque des nouvelles données deviennent disponibles, par conséquent, Profil Technology et Bitdefender recommandent que vous consultiez régulièrement notre site "Produits" à l'adresse suivante : http://www.bitdefender.fr pour des mises à jour, ou notre site internet de FAQ à l'adresse http://www.bitdefender.fr/site/KnowledgeBase/supportCenter/.

Tout dommage direct, indirect, spécial, accidentel ou conséquent en relation avec l'usage des informations fournies ne peuvent pas être imputés à Profil Technology et Bitdefender.

Si une intervention sur site est nécessaire, l'analyste vous donnera de plus amples instructions concernant votre revendeur le plus proche.

35. RESSOURCES EN LIGNE

De nombreuses ressources en ligne sont disponibles pour vous aider à résoudre vos questions et problèmes liés à Bitdefender.

Centre de Support de Bitdefender :

http://www.bitdefender.fr/support/consumer.html

Forum du Support Bitdefender :

http://forum.bitdefender.com/index.php?showforum=59

le portail de sécurité informatique Bitdefender blog :

http://www.bitdefender.fr/blog/

Vous pouvez également utiliser votre moteur de recherche favori pour obtenir plus d'informations sur la sécurité informatique, les produits et l'entreprise Bitdefender.

35.1. Centre de Support de Bitdefender

Le Centre de Support de Bitdefender est une base en ligne d'informations concernant les produits Bitdefender. Il contient, dans un format facilement accessible, les rapports d'incidents survenus et constatés par le support technique, les équipes de réparation des bugs de Bitdefender. Ainsi que des articles généraux sur la prévention antivirus, la gestion des solutions Bitdefender, des informations détaillées et beaucoup d'autres articles.

Le Centre de Support de Bitdefender est accessible au public et consultable gratuitement. Cet ensemble d'informations est une autre manière de fournir aux clients de Bitdefender les informations techniques dont ils ont besoin. Toutes les requêtes valides d'informations ou de rapports de bugs provenant de clients Bitdefender trouvent une réponse dans le Centre de Support Bitdefender, comme les rapports de corrections de bugs, les solutions de rechange, ou les articles d'informations venant compléter les fichiers d'aide des produits.

Le Centre de Support de Bitdefender est disponible en permanence sur

http://www.bitdefender.fr/support/consumer.html.

35.2. Forum du Support Bitdefender

Le Forum du Support Bitdefender fournit aux utilisateurs de Bitdefender une manière simple d'obtenir de l'aide et d'aider les autres.

Si votre produit Bitdefender ne fonctionne pas correctement, s'il ne peut pas supprimer certains virus de votre ordinateur ou si vous avez des questions sur son mode de fonctionnement, exposez votre problème ou posez vos questions sur le forum.

Les techniciens du support Bitdefender surveillent le forum à la recherche de nouvelles publications afin de vous aider. Vous pouvez également obtenir une réponse ou une solution d'un utilisateur Bitdefender plus expérimenté.

Avant de publier un problème ou une question, recherchez s'il existe une rubrique similaire ou connexe dans le forum.

Le forum de support de Bitdefender est disponible à http://forum.bitdefender.com/index.php?showforum=59, dans 5 langues différentes: français, anglais, allemand, espagnol et roumain. Cliquez sur le lien **Protection des indépendants & des petites entreprises** pour accéder à la section dédiée aux produits de consommation.

35.3. Bitdefender blog

Bitdefender blog comprend de nombreuses informations sur la sécurité informatique. Vous pouvez découvrir ici les différentes menaces auxquelles votre ordinateur est exposé lorsqu'il est connecté à Internet (malwares, phishing, spam, cybercriminels).

De nouveaux articles sont régulièrement publiés pour vous tenir au courant des dernières menaces découvertes, des tendances actuelles en matière de sécurité et vous fournir encore d'autres informations sur le secteur de la sécurité informatique.

La page web de Bitdefender blog est http://www.bitdefender.fr/blog/.

36. NOUS CONTACTER

Une communication efficace est la clé d'une relation réussie. Au cours des dix dernières années, BITDEFENDER s'est bâti une réputation incontestable dans sa recherche constante d'amélioration de la communication pour dépasser les attentes de ses clients et de ses partenaires. N'hésitez pas à nous contacter pour toute question.

36.1. Adresses Web

Ventes : bitdefender@profiltechnology.com
Centre de support :http://www.bitdefender.fr/support/consumer.html
Documentation : documentation@bitdefender.com
Distributeurs locaux : http://www.bitdefender.fr/partenaires/
Programme de partenariat : partners@bitdefender.com
Relations médias : pr@bitdefender.com
Emplois : jobs@bitdefender.com
Soumissions de virus : virus_submission@bitdefender.com
Envoi de spams : spam_submission@bitdefender.com
Signaler un abus : abuse@bitdefender.com
Site web : http://www.bitdefender.fr

36.2. Distributeurs locaux

Les distributeurs locaux Bitdefender se tiennent prêts à répondre à vos questions concernant leur zone d'opération, à propos de sujets commerciaux ou généraux.

Pour trouver un distributeur Bitdefender dans votre pays :

1. Allez à http://www.bitdefender.fr/partenaires/.
2. Cliquez sur l'onglet **Trouver un partenaire**.
3. Les informations de contact des distributeurs locaux de Bitdefender devraient s'afficher automatiquement. Si ce n'est pas le cas, sélectionnez votre pays de résidence pour afficher les informations.
4. Si vous ne trouvez pas de distributeur Bitdefender dans votre pays, n'hésitez pas à nous contacter par e-mail à l'adresse bitdefender@profiltechnology.com. Merci de nous contacter par email pour optimiser le traitement de votre demande.

36.3. Bureaux de Bitdefender

Les bureaux de Bitdefender se tiennent prêts à répondre à vos questions concernant leur zone d'opération, à propos de sujets commerciaux ou généraux. Leur adresse respective et contacts sont listés ci-dessous.

France

Profil Technology
49, Rue de la Vanne
92120 Montrouge
Téléphone : +33 (0)1 47 35 72 73
Ventes : bitdefender@profiltechnology.com
Soutien technique : http://www.bitdefender.fr/site/Main/nousContacter
Site Web : http://www.bitdefender.fr

U.S.A

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
Téléphone (services administratif et commercial) : 1-954-776-6262
Ventes : sales@bitdefender.com
Soutien technique : http://www.bitdefender.com/support/consumer.html
Site Web : http://www.bitdefender.com

Royaume-Uni et Irlande

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
E-mail : info@bitdefender.co.uk
Téléphone : +44 (0) 8451-305096
Ventes : sales@bitdefender.co.uk
Soutien technique : http://www.bitdefender.com/support/consumer.html
Site Web : http://www.bitdefender.co.uk

Allemagne

Bitdefender GmbH
TechnoPark Schwerte

Lohbachstrasse 12
D - 58239 Schwerte
Deutschland
Service administratif : +49 2304 9 45 - 162
Fax : +49 2304 9 45 - 169
Ventes : vertrieb@bitdefender.de
Soutien technique : http://www.bitdefender.de/support/consumer.html
Site Web : http://www.bitdefender.de

Espagne

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax : +34 93 217 91 28
Téléphone : +34 902 19 07 65
Ventes : comercial@bitdefender.es
Soutien technique : http://www.bitdefender.es/support/consumer.html
Site Internet : http://www.bitdefender.es

Roumanie

BITDEFENDER SRL
Complex DV24, Building A, 24 Delea Veche Street, Sector 2
Bucharest
Fax : +40 21 2641799
Téléphone du service commercial : +40 21 2063470
Email du service commercial : sales@bitdefender.ro
Soutien technique : http://www.bitdefender.ro/support/consumer.html
Site Internet : http://www.bitdefender.ro

Émirats arabes unis

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Téléphone du service commercial : 00971-4-4588935 / 00971-4-4589186
Email du service commercial : sales@bitdefender.com
Soutien technique : http://www.bitdefender.com/support/consumer.html
Site Internet : http://www.bitdefender.com/world

Glossaire

ActiveX

ActiveX est un modèle pour écrire des programmes afin que d'autres programmes et le système d'exploitation puissent les appeler. La technologie ActiveX est utilisée par Microsoft Internet Explorer pour créer des pages Web interactives qui ressemblent et se comportent comme des programmes informatiques classiques, plutôt que comme des pages statiques. Avec ActiveX, les utilisateurs peuvent poser ou répondre à des questions, utiliser des boutons et interagir de multiples façons avec les pages Web. Les commandes ActiveX sont souvent écrites en Visual Basic.

Active X est connu pour son manque total de commandes de sécurité ; les experts en sécurité informatique déconseillent son utilisation sur Internet.

Applet Java

Il s'agit d'un programme Java conçu pour s'exécuter uniquement dans une page Web. Pour utiliser un applet dans une page Web, vous devez spécifier le nom de l'applet et la taille (la longueur et la largeur - en pixels) qu'il peut utiliser. Lors d'un accès à la page Web, le navigateur télécharge l'applet depuis un serveur et l'exécute sur la machine de l'utilisateur (le client). Les applets diffèrent des applications par le fait qu'ils sont régis par un protocole de sécurité strict.

Par exemple, bien que les applets s'exécutent sur le client, ils ne peuvent pas lire ou écrire des données sur la machine du client. De plus, les applets sont également limités pour ne pouvoir lire et écrire des données que depuis le domaine les hébergeant.

Archive

Une disquette, une bande ou un répertoire contenant des fichiers qui ont été sauvegardés.

Un fichier qui contient un ou plusieurs fichiers dans un format compressé.

Chemin

Directions exactes vers un fichier d'un ordinateur. Ces directions sont généralement décrites par arborescence, de haut en bas.

La connexion entre deux points, comme le canal de communication entre deux ordinateurs.

Client de messagerie

Un client de messagerie est un logiciel qui vous permet d'envoyer et recevoir des messages (courriels).

Courriel

Courrier électronique. Il s'agit d'un service d'envoi de messages sur des ordinateurs via un réseau local ou global.

Dossier de démarrage

Tous les fichiers placés dans ce dossier s'ouvrent au démarrage de l'ordinateur. Par exemple, un écran de démarrage, un fichier son pour le démarrage de l'ordinateur, un calendrier, des programmes, peuvent être placés dans ce dossier. C'est généralement un raccourci vers le fichier qui est placé dans le dossier, et pas le fichier.

Enregistreur de frappe

Application qui enregistre tout ce qui est tapé.

Les enregistreurs de frappe ne sont pas nécessairement malveillants. Ils peuvent être utilisés à des fins légitimes, comme pour surveiller les activités d'employés ou d'enfants. Ils sont toutefois de plus en plus utilisés par les cybercriminels à des fins malveillantes (par exemple, pour recueillir des informations confidentielles, telles que des identifiants de connexion ou des numéros de sécurité sociale).

Événements

Il s'agit d'une action ou d'une occurrence détectée par un programme. Les événements peuvent être des actions d'utilisateur, comme le clic sur un bouton de souris ou la pression d'une touche, ou des occurrences du système, comme le manque de mémoire.

Extension de fichier

La partie d'un fichier, après le point final, qui indique le type de données stockées dans le fichier.

De nombreux systèmes d'exploitation utilisent des extensions de fichiers, par exemple Unix, VMS, MS-DOS. Elles comportent communément une à trois lettres (certains vieux systèmes n'en supportent pas plus de trois).

Exemples: "c" pour du code source en C, "ps" pour PostScript, "txt" pour du texte.

Fausse alerte
Se produit lorsqu'une analyse identifie un fichier comme infecté alors qu'il ne l'est pas.

Fichier journal (Log)
Fichier qui enregistre les actions ayant eu lieu. Bitdefender maintient un fichier journal contenant les chemins analysés, les dossiers, le nombre d'archives et de fichiers analysés, le nombre de fichiers suspects et infectés.

Hameçonnage
Action d'envoyer un courriel à un utilisateur en prétendant être une entreprise connue dans le but d'obtenir frauduleusement des informations privées qui permettront d'utiliser l'identité du destinataire du courriel. Cet courriel oriente l'utilisateur vers un site Web où il lui est demandé de mettre à jour des informations personnelles, comme ses mots de passe, son numéro de carte de crédit, de sécurité sociale ou de compte en banque, que les véritables entreprises connaissent déjà. Ce site Web est bien sûr totalement factice et n'a pour objectif que de voler les informations de l'utilisateur.

Heuristique
Méthode basée sur des règles permettant d'identifier de nouveaux virus. Cette méthode d'analyse ne s'appuie pas sur des définitions virales spécifiques. L'avantage de l'analyse heuristique est de pouvoir détecter les variantes d'un virus existant. Cependant, cette méthode peut parfois occasionner de fausses alertes dans des programmes normaux.

IP
Protocole Internet - Un protocole routable de la suite de protocoles TCP/IP chargé de l'adressage, du routage IP et de la fragmentation et réassemblage des paquets IP.

Lecteur de disque
C'est un appareil qui lit et écrit des données sur un disque.

Une unité de disque dur lit et écrit sur un disque dur.

Un lecteur de disquette accède à des disquettes.

Les lecteurs peuvent être soit internes (intégrés à un ordinateur) soit externes (intégrés dans un boîtier séparé que l'on connecte à l'ordinateur).

Ligne de commande

Dans une interface en ligne de commande, l'utilisateur tape directement des commandes correspondant à des ordres de gestions.

Logiciel espion

Tout type de logiciel récupérant les informations des utilisateurs via leur connexion Internet à leur insu, généralement à des fins publicitaires. Les logiciels espions sont généralement cachés dans des partagiciels et logiciels gratuits pouvant être téléchargés sur Internet. Notons toutefois que la plupart des partagiciels et logiciels gratuits ne contiennent pas de logiciels espions. Une fois installé, le logiciel espion surveille l'activité de l'utilisateur sur Internet et transmet discrètement ces informations à une tierce personne. Les logiciels espions peuvent également récupérer des informations sur les adresses courriel, les mots de passe ou même, les numéros de cartes de crédit.

Leur point commun avec les chevaux de Troie est le fait que les utilisateurs les installent involontairement en même temps qu'un autre produit. Une des manières les plus classiques d'être victime de logiciels espions est de télécharger des logiciels de partage de fichiers (Peer to peer).

En plus des questions d'éthique et de respect de la vie privée, les logiciels espions volent les ressources de l'ordinateur de l'utilisateur en utilisant sa bande passante lors de l'envoi d'informations à leur base via la connexion Internet. En raison de cette utilisation de la mémoire et des ressources du système, les applications qui fonctionnent en tâche de fond peuvent aller jusqu'à entraîner des plantages ou provoquer une instabilité globale du système.

Mémoire

Zones de stockage internes dans l'ordinateur. Le terme mémoire définit le stockage de données sous la forme de composants électroniques, le mot stockage étant utilisé pour définir le stockage de données sur bande magnétique ou disques amovibles. Chaque ordinateur a une certaine quantité de mémoire physique, appelée mémoire vive ou RAM.

Mise à jour

Nouvelle version d'un logiciel ou d'un produit hardware, destinée à remplacer une version antérieure du même produit. Habituellement, les installations de mises à jour vérifient si le produit initial est installé, et si ce n'est pas le cas, la mise à jour ne se fait pas.

Bitdefender a son propre module de mise à jour permettant à l'utilisateur de vérifier manuellement les mises à jour ou de les programmer automatiquement.

Navigateur

Raccourci pour navigateur internet, il s'agit d'un logiciel utilisé pour visualiser des pages Web. Les principaux navigateurs comprennent Microsoft Internet Explorer, Mozilla Firefox et Google Chrome. Ce sont des navigateurs graphiques, ce qui signifie qu'ils peuvent afficher aussi bien le graphisme que le texte. De plus, les navigateurs les plus modernes peuvent visionner les informations multimédia, y compris le son et la vidéo, bien qu'ils exigent des modules d'extension (plugins) pour certains formats.

Non heuristique

Cette méthode d'analyse utilise les définitions spécifiques des virus. L'avantage de l'analyse non-heuristique est qu'elle n'est pas trompée par ce qui peut sembler être un virus et ne génère donc pas de fausses alertes.

Photon

Photon est une technologie Bitdefender innovante et discrète, conçue pour limiter l'impact de la protection antivirus sur les performances. En surveillant l'activité de votre PC en tâche de fond, elle crée des modèles d'utilisation qui aident à optimiser les processus de démarrage et d'analyse.

Port

Une interface sur un ordinateur auquel vous pouvez connecter un appareil. Les ordinateurs comportent plusieurs sortes de ports. Il existe plusieurs ports internes permettant de connecter des lecteurs de disques, des écrans et des claviers. A l'extérieur, les ordinateurs ont des ports pour connecter des modems, imprimantes, souris et autres périphériques.

Dans des réseaux TCP/IP et UDP, un point final pour une connexion logique. Le numéro du port identifie son type. Par exemple, le port 80 est utilisé pour le trafic HTTP.

Portes dérobées

Il s'agit d'une faille dans la sécurité d'un système délibérément laissée en place par des développeurs ou des personnes chargées de la maintenance. Les intentions ne sont pas toujours malveillantes ; quelques systèmes d'exploitation, par exemple, permettent à des techniciens de maintenance, via des comptes privilégiés, de prendre le contrôle à distance.

Pourriel

Messages électroniques ou messages de groupes de discussion indésirables. Souvent répertoriés comme des courriels non sollicités.

Programmes empaquetés

Fichier dans un format compressé. Beaucoup de systèmes d'exploitation et d'applications contiennent des commandes vous permettant de compresser un fichier afin qu'il occupe moins de mémoire. Par exemple, imaginons que vous avez un fichier texte contenant dix caractères "espace vide" à la suite. Normalement, cela nécessite 10 octets.

Pourtant, un logiciel qui compresse des fichiers remplace la série d'espaces par un caractère spécial pour les séries d'espaces suivi du nombre d'espaces remplacés. Dans ce cas, les dix espaces nécessitent seulement 2 octets. Il s'agit d'une technique de compression - il en existe plusieurs autres.

Publiciels

Les publiciels sont souvent associés à des applications gratuites mais exigeant leur acceptation par l'utilisateur. Ces publiciels étant généralement installés une fois que l'utilisateur en a accepté le principe dans un accord de licence, ils ne peuvent pas être considérés comme illégaux.

Cependant, les fenêtres publicitaires peuvent devenir contrariantes et, dans certains cas, dégrader les performances du système. De plus, les informations collectées peuvent mettre en péril la vie privée des utilisateurs qui ne s'étaient pas complètement rendu compte des termes de l'accord de licence.

Rootkit

Un rootkit est un ensemble d'outils logiciels permettant un accès de niveau administrateur à un système. Le terme a été utilisé initialement pour les systèmes d'exploitation UNIX et se réfère à des outils recompilés fournissant des droits administrateurs "intrusifs", permettant de cacher leur présence aux administrateurs système.

Le principal rôle des rootkits est de masquer des processus, des fichiers, des sessions et des journaux. Ils peuvent également intercepter des données depuis des terminaux, des connexions réseau ou des périphériques, s'ils incluent les logiciels appropriés.

Les rootkits ne sont pas nécessairement malveillants. Par exemple, les systèmes d'exploitation et même certaines applications cachent des fichiers sensibles en utilisant des rootkits. Cependant, ils sont principalement utilisés pour camoufler des codes malveillants ou pour cacher la présence d'un intrus sur le système. Lorsqu'ils sont combinés à des codes malveillants, les rootkits sont une menace importante contre l'intégrité et la sécurité d'un système. Ils peuvent analyser le trafic, créer des portes dérobées sur le système, modifier des fichiers et des journaux et passer inaperçus.

Scripts

Autre terme pour macro ou fichier batch, un script est une liste de commandes qui peut être exécutée sans intervention utilisateur.

Secteur d'amorçage

Secteur au début de chaque disque qui identifie l'architecture du disque (taille des secteurs, du cluster, etc). Pour les disques de démarrage, le secteur d'amorçage contient aussi un programme qui charge le système d'exploitation.

Signature de virus

La "signature" binaire du virus, utilisé par l'antivirus pour la détection et l'élimination du virus.

TCP/IP

Transmission Control Protocol/Internet Protocol - Ensemble de protocoles réseau utilisés largement sur Internet assurant la communication entre des réseaux interconnectés d'ordinateurs avec diverses architectures matérielles et divers systèmes d'exploitation.

TCP/IP inclut des standards pour la communication des ordinateurs et des conventions pour la connexion des réseaux et le routage du trafic.

Télécharger

Copie des données (généralement un fichier entier) d'une source principale vers un dispositif périphérique. Le terme est souvent utilisé pour décrire le processus de copie d'un fichier d'un service en ligne vers son ordinateur. Le téléchargement peut aussi se référer à la reproduction d'un fichier d'un serveur de réseau vers un ordinateur sur le réseau.

Cookies

Sur Internet, les cookies sont définis comme étant de petits fichiers contenant des informations sur les ordinateurs individuels qui peuvent être analysés et utilisés par des annonceurs publicitaires pour tracer vos centres d'intérêts et vos goûts. Dans ce milieu, la technologie des cookies est encore en développement et l'intention est de cibler directement ce que vous avez dit être vos intérêts. C'est une arme à double tranchant pour beaucoup de personnes parce que d'une part, c'est efficace et pertinent car vous voyez seulement les annonces vous intéressant. Mais cela implique également le "pistage" et le "suivi" des sites que vous consultez et de ce sur quoi vous cliquez. Il y a naturellement un débat sur la vie privée et beaucoup de gens se sentent ainsi considérés comme un simple "code SKU" (ce code barres se trouvant au dos des produits de consommation). Bien que ce point de vue puisse paraître extrême, il est parfois justifié.

Trojan (cheval de Troie)

Programme destructeur qui prétend être une application normale. Contrairement aux virus, les chevaux de Troie ne se répliquent pas, mais ils peuvent être tout aussi destructeurs. Un des types de chevaux de Troie les plus insidieux est un logiciel qui prétend désinfecter votre PC mais qui au lieu de cela l'infecte.

Le terme provient de la fameuse histoire de l'Iliade écrite par Homère, dans laquelle les Grecs font un cadeau de "paix" à leurs ennemis, les Troyens, un immense cheval en bois. Ce n'est qu'après avoir fait entrer le cheval dans leur ville qu'ils se rendent compte que le cheval est plein de soldats grecs, qui ouvrent les portes de la ville, permettant aux attaquants de capturer Troie.

Ver

Programme qui se propage tout seul en réseau, se reproduisant au fur et à mesure de sa propagation. Il ne peut pas se joindre à d'autres programmes.

Virus

Programme ou morceau de code chargé dans votre ordinateur à votre insu et qui fonctionne contre votre gré. La plupart des virus peuvent également se répliquer. Tous les virus informatiques sont créés par des personnes. Un virus simple peut se copier très rapidement et sans arrêt et est relativement facile à créer. Même un virus simple comme celui décrit est dangereux puisqu'il remplit vite la mémoire et bloque le système. Un virus plus dangereux encore est par exemple capable de se transmettre via un réseau et de déjouer les systèmes de sécurité.

Virus d'amorçage

Virus qui infecte le secteur d'amorçage d'une disquette ou d'un disque dur. Une tentative de démarrer depuis une disquette infectée avec un virus d'amorçage rendra le virus actif en mémoire. Chaque fois que vous démarrez votre système depuis ce point, vous aurez le virus actif en mémoire.

Virus Macro

Type de virus codé sous la forme d'une macro intégrée dans un document. Beaucoup d'applications, telles Microsoft Word et Excel, supportent de puissants langages macro.

Ces applications vous permettent d'intégrer une macro dans un document, et de le faire s'exécuter chaque fois que le document est ouvert.

Virus polymorphe

Virus qui change de forme avec chaque fichier qu'il infecte. Ces virus n'ayant pas de forme unique bien définie, ils sont plus difficiles à identifier.

Zone de notification

Introduite avec Windows 95, la zone de notification se situe dans la barre de tâches Windows (en général, à côté de l'horloge) et contient des icônes miniatures permettant d'accéder facilement aux fonctions

système : télécopieur, imprimante, modem, volume, etc. Double-cliquez ou faites un clic-droit sur une icône pour afficher les options.